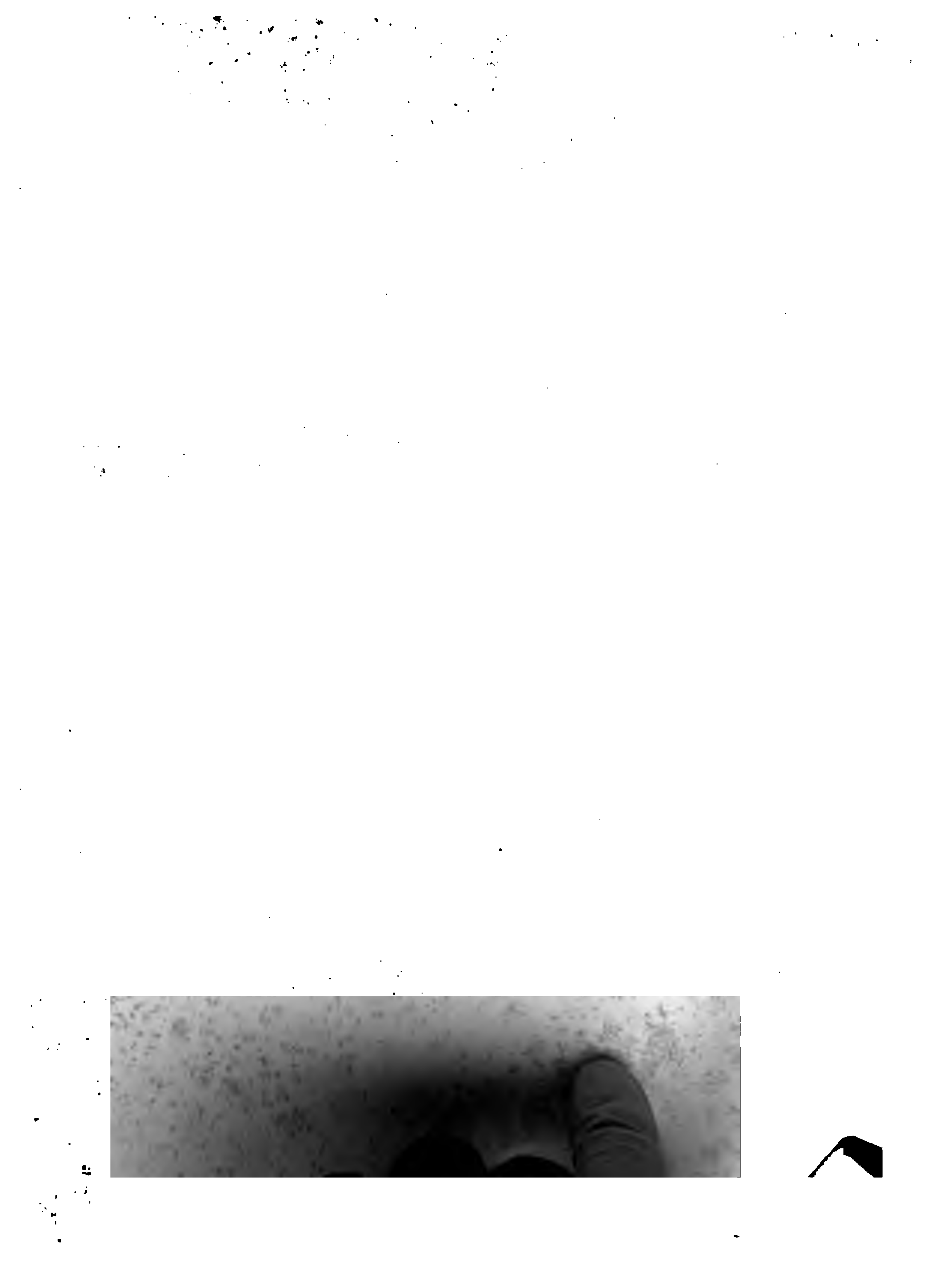




GRUNDZÜGE EINER ARITHMETISCHEN THEORIE DER ALGEBRAISCHEN GRÖSSEN.

FESTSCHRIFT

ZU

HERRN ERNST EDUARD KUMMER'S

FÜNFZIGJÄHRIGEM DOCTOR-JUBILÄUM,

10. SEPTEMBER 1881,

VON

L. KRONECKER.

ANGEFÜGT IST EINE NEUE AUSGABE DER AM 10. SEPT. 1845 ERSCHIENENEN INAUGURAL-DISSERTATION DE UNITATIBUS COMPLEXIS

BERLIN.
DRUCK UND VERLAG VON G. REIMER.
1882.

GRUNDZÜGE EINER ARITHMETISCHEN THEORIE DER ALGEBRAISCHEN GRÖSSEN.

HERRN ERNST EDUARD KUMMER

zum 10. September 1881.

Lieber Freund! Seit siebenundvierzig Jahren Dein Schüler und beinahe ebenso lange Dein Freund, glaube ich mich berechtigt, zu Deinem Doctor-Jubiläum diese Festschrift zu veröffentlichen. Ihr Inhalt weniger als ihre Bestimmung motivirt wohl auch die Anfügung einer neuen, vollständigen Ausgabe meiner Doctor-Dissertation, welche Dir am 10. September 1845 von mir gewidmet, aber damals nicht bis zu Ende abgedruckt worden ist. Beide Arbeiten berichten auf ihren Blättern von dem, was ich Dir verdanke. Aber nur unvollkommen. In Wahrheit verdanke ich Dir mein mathematisches Dasein; ich verdanke Dir in der Wissenschaft, der Du mich früh zugewendet, wie in der Freundschaft, die Du mir früh entgegengebracht hast, einen wesentlichen Theil des Glückes meines Lebens.

LEOPOLD KRONECKER.

Inhalts-Verzeichniss.

Seite

Grundzüge einer arithmetischen Theorie der algebraischen Grössen. 1—122

I. Theil.

II. Theil.

Gleichzeitige Beschäftigung mit algebraischen und zahlentheoretischen Studien hat mich schon früh dazu geleitet, die arithmetische Seite der Algebra besonders ins Auge zu fassen. So führte mich die Untersuchung der aus Wurzeln *Abel*scher Gleichungen gebildeten complexen Zahlen auf jenes algebraisch-arithmetische Problem, alle *Abel*schen Gleichungen für irgend einen Rationalitäts-Bereich aufzustellen, dessen Lösung ich im Juni 1853 der hiesigen Akademie mitgetheilt habe. Seitdem habe ich stets in gedruckten Publicationen wie in meinen Universitäts-Vorlesungen die arithmetischen Gesichtspunkte in der Algebra besonders hervorgehoben und auch vielfach die arithmetischen Methoden auf einzelne algebraische Fragen angewendet. Doch war es mir kaum möglich, über diese meine Arbeiten Mittheilung zu machen, ohne mich auf die allgemeine Theorie berufen zu können, und ich habe mich desshalb seit längerer Zeit mit dem Gedanken getragen, eine ausführliche Arbeit darüber zu veröffentlichen. Aber mannigfache Hindernisse, vor Allem der Wunsch die vielen noch vorhandenen Lücken der Untersuchung auszufüllen, haben mich davon zurückgehalten, bis jetzt der Wunsch überwog, meinem Freunde und Lehrer zu seinem Festtage die Ergebnisse anhaltender Forschungen gesammelt und geordnet darzubringen, obgleich ich mir beim Anfange ebenso der Schwierigkeit meines Vorhabens wie nachher beim Abschlusse der Unvollkommenheit des Werkes bewusst gewesen bin.

Da der Umfang der Arbeit über das Maass einer Abhandlung angewachsen ist, habe ich sie der Uebersicht wegen in zwei Theile gesondert. In dem ersten werden die weiteren und engeren Sphären der Existenz der algebraischen Grössen fixirt, es wird die Art ihrer Existenz genauer dargelegt und zwar auch in dem Falle, wo mehrere derselben zugleich durch irgend

eine Anzahl algebraischer Gleichungen definirt oder eigentlich nur gefordert werden. Im zweiten Theile werden die arithmetischen Eigenschaften der *ganzen* algebraischen Grössen, d. h. diejenigen, welche auf ihre Theilbarkeit Bezug haben, entwickelt. — Während im ersten Theile von der unendlichen Menge algebraischer Grössen einer Sphäre ausgegangen wird und ihre zunächst nur begriffliche Zusammenfassung in Gattungen und Arten durch eine gemeinschaftliche Darstellung concreten Ausdruck erhält, wird im zweiten Theile von einer beliebigen endlichen Anzahl ganzer algebraischer Grössen ausgegangen und dem zunächst nur durch Analogie mit den ganzen rationalen Grössen geforderten Begriffe des gemeinsamen Theilers durch einen algebraischen Ausdruck entsprochen. Wie jener elementareren Aufgabe der Darstellung aller ganzen algebraischen Grössen einer Gattung nur dadurch genügt werden konnte, dass an die Stelle ganzer Functionen *einer* algebraischen Grösse lineare Functionen von mehreren genommen, d. h. dass den Potenzen einer einzigen algebraischen Grösse noch andere Elemente der Gattung associirt wurden, um die gebrochenen „idealen" Grössen zu wirklichen zu machen*), so erforderte das höhere Problem der Darstellung des gemeinschaftlichen Theilers ganzer algebraischer Grössen die Association der „ganzen algebraischen Formen", um diesen aus der Sphäre blosser Abstraction in die Wirklichkeit algebraischer Gebilde zu versetzen. Aus der Vereinigung dieser beiden Darstellungs-Principien werden im Schlussparagraphen die Fundamentalgleichungen hergeleitet, mit Hülfe deren sich die gesammte Theorie der algebraischen Grössen auf die der rationalen Functionen von Variabeln reduciren lässt, und da bei dieser Reduction sich die Anzahl der Variabeln und die Stufenzahl der Formen erhöht, so zeigt sich, dass jener mit den Formen selbst zugleich eingeführte Begriff ihrer verschiedenen Stufen den Begriff der algebraischen Irrationalität zu ersetzen geeignet ist.

Dass viele zum Thema gehörige Fragen noch unerledigt geblieben, viele behandelte Punkte näher auszuführen sind, habe ich an den einzelnen Stellen der Arbeit selbst hervorgehoben und schon durch den Titel angedeutet. Ich habe hier nur die „Grundzüge" einer im Wesentlichen neuen Behandlungsweise der algebraischen Grössen geben wollen oder können.

---

*) Diese Darstellungsweise hat in dem speciellen Falle der algebraischen Zahlen auch Herr *Dedekind* angewendet und vor mir 1871 durch den Druck veröffentlicht (vgl. die Vorbemerkung zu meiner Abhandlung im Journ. f. Math. Bd. 91, S. 301). Die Bedeutung gebrochener idealer Zahlen ist schon auf S. 31 der *Kummer*schen Abhandlung „Ueber die allgemeinen Reciprocitätsgesetze" aus dem Jahre 1859 dargelegt.

Erster Theil.

§ 1.

Die Rationalitäts-Bereiche.

Ich fixire, wie in meinen früheren Aufsätzen, z. B. in denjenigen, welche in den Monatsberichten der Berliner Akademie vom Juni 1853, vom Februar 1873 und vom März 1879 abgedruckt sind, durch die Grössen $\mathfrak{R}'$, $\mathfrak{R}''$, $\mathfrak{R}'''$, ... einen bestimmten Rationalitäts-Bereich $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$. In dem ersten von jenen erwähnten Aufsätzen sind die den Rationalitäts-Bereich charakterisirenden Grössen mit $A, B, C, \ldots$ bezeichnet. Die dort zuerst eingeführte Fixirung eines solchen Bereichs war, wie a. a. O. näher dargelegt ist, für die Klärung der Theorie der algebraischen Gleichungen durchaus nothwendig. Das Bedürfniss einer Präcisirung dessen, was bei einer bestimmten Untersuchung als rational zu betrachten sei, tritt bei *Galois* und auch schon bei *Abel*, namentlich in der Einleitung zu seinem unvollendeten Aufsatze „sur la résolution algébrique des équations“ (Oeuvres complètes, Tome II p. 185), deutlich hervor. Doch geht *Abel* in seinen betreffenden Ausführungen, wie sich dann zeigt, nicht bis auf das nothwendige Fundament rationaler Functionen mit ganzzahligen Coefficienten zurück, sondern behält im Gegentheil die nähere Bestimmung der Coefficienten vor, und bei *Galois* macht die weitere Entwickelung die Präcisirung des „Rationalen“ überflüssig. In dem letzten meiner oben erwähnten Aufsätze habe ich, wie auch stets in meinen Universitäts-Vorlesungen, den Ausdruck „Rationalitäts-Bezirk“ gebraucht, um dessen in gewisser Hinsicht willkürliche Abgrenzung zu kennzeichnen; doch glaube ich den hier gewählten Ausdruck „Bereich“ um desswillen vorziehen zu sollen, weil darin der Begriff des Räumlichen weniger scharf ausgeprägt ist, und weil er sich in Folge dessen den anderen in meinen Arbeiten und Universitäts-Vorlesungen eingeführten, durchweg nach *Gauss*' klassischem Muster der Systematik der beschreibenden Naturwissenschaften entlehnten Bezeichnungen näher anschliesst. Ueberdies findet sich auch im gewöhnlichen Sprachgebrauch bei dem Begriffe eines „Bereichs“ die Möglichkeit einer verschiedenen Abgrenzung nicht geradezu ausgeschlossen, wenn sie auch darin weniger — als in dem Ausdruck „Bezirk“ — hervorgehoben ist.

Der Rationalitäts-Bereich $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$ enthält, wie schon die Bezeichnung deutlich erkennen lässt, alle diejenigen Grössen, welche rationale Functionen der Grössen $\mathfrak{R}'$, $\mathfrak{R}''$, $\mathfrak{R}'''$, ... mit ganzzahligen Coefficienten sind. Diese Bestimmung, dass die Coefficienten ganzzahlig sein sollen, ist nur hier im Anfange, um jedes Missverständniss auszuschliessen, hinzugefügt. Im Folgenden soll stets, wie in allen meinen früheren Aufsätzen, der Begriff „der rationalen Function der Grössen $\mathfrak{R}$“, auch ohne weitere Hinzufügung, in seiner ursprünglichen, einzig präcisen Bedeutung als der einer rationalen Function mit ganzzahligen Coefficienten gebraucht werden. Wenn an einzelnen Stellen der Untersuchung bei rationalen Functionen der Grössen $\mathfrak{R}$ von der Beschaffenheit der Coefficienten abgesehen werden soll, so ist es geeigneter, sie als solche zu bezeichnen, welche die Elemente $\mathfrak{R}$ in rationaler Weise enthalten oder durch rationale Operationen aus denselben gebildet sind.

Durch den „Rationalitäts-Bereich $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$“ sollen die sämmtlichen rationalen Functionen der Elemente $\mathfrak{R}$ — nur zur Erleichterung der Ausdrucksweise bei der Darstellung der Theorie — begrifflich zusammengefasst werden, und in derselben Weise soll auch noch weiterhin die Einordnung von „Grössen“ nach bestimmten, besonders darzulegenden, gemeinsamen Eigenschaften in geschlossene Kreise oder Kategorieen erfolgen. Der Ausdruck „Grösse“ ist hierbei in der weitesten arithmetisch-algebraischen Bedeutung zu nehmen, und es sind im Allgemeinen auch Grössengebilde wie „rationale Functionen unbestimmter Grössen“, sogenannte „Formen beliebig vieler Veränderlicher“ u. s. w. mit darunter zu verstehen, denen der Begriff der Maassgrösse, der des „grösser oder kleiner Seins“ gänzlich fremd ist. Aber die gewöhnlichen Zahlengrössen, die rationalen wie die algebraischen irrationalen Zahlen, gehören mit in die Kategorie der zu behandelnden Grössen, und es ist desshalb ausdrücklich hervorzuheben, dass, obgleich hier das „grösser oder kleiner Sein“ volle Bedeutung hat, dennoch bei allen im Folgenden vorkommenden Gruppirungen, weil sie nach allgemeineren Gesichtspunkten vorzunehmen sind, die Maassgrösse keinerlei Rücksicht bilden wird. Bei der in § 3 erfolgenden Einführung des Gattungsbegriffs liegt z. B. die zu einer besonderen Gattung gehörige Grösse $\sqrt{2}$ *„begrifflich“* weit ab von irgend einer der Quadratwurzel aus *zwei* noch so nahe liegenden rationalen Zahl; ebenso tritt bei der späteren Unterscheidung der ganzen und gebrochenen Zahlen für die der Grösse nach benachbarten

Zahlen der beiden Kategorieen eine begriffliche Trennung ein. Eben desshalb, und weil man doch gewohnt ist, sich die Zahlengrössen ihrer Maassgrösse nach, nicht aber ihren algebraischen Eigenschaften nach, an einander gereiht oder irgend wie räumlich gruppirt vorzustellen, halte ich es für angemessen, in der Terminologie die Ausdrücke mit entschieden räumlichem Gepräge zu vermeiden und nur solche, kaum zu umgehende allgemeine Ausdrücke — wie eben jenes Wort „Bereich" — oder allgemeine Bilder zu gebrauchen, welche die ursprünglich räumliche Bedeutung bei ihrer vielfachen Verwendung im gewöhnlichen Sprachgebrauche schon fast verloren haben. Aus diesem Gesichtspunkte habe ich auch geglaubt, von der Adoption der *Dedekind*schen Bezeichnung „Körper" absehen und meine ältere Bezeichnungsweise im Wesentlichen beibehalten zu sollen, zumal gerade — wenigstens für die vorliegenden Untersuchungen — mir eine ganz neue Begriffsbildung zur Zusammenfassung der rationalen Functionen bestimmter Grössen $\mathfrak{R}'$, $\mathfrak{R}''$, $\mathfrak{R}'''$, ... nicht erforderlich und diese Zusammenfassung selbst durch das Wort „Rationalitäts-Bereich" in schlichter, ungezwungener Weise ausdrückbar erschien.

Mit der Fixirung des Rationalitäts-Bereichs wird die Frage der Zerlegbarkeit ganzer Functionen von einer oder mehreren Veränderlichen, deren Coefficienten jenem Bereich angehören, zu einer völlig bestimmten, insofern dabei verlangt wird, dass auch die Coefficienten der Factoren eben demselben Bereich angehören sollen. In diesem Sinne soll nun stets eine ganze Function von beliebig vielen Veränderlichen mit Coefficienten aus dem Rationalitäts-Bereich $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$ schlechthin als „irreductibel" oder „unzerlegbar" bezeichnet werden, wenn sie keine eben solche ganze Function, d. h. keine ganze Function derselben Veränderlichen mit Coefficienten aus demselben Rationalitäts-Bereich als Factor enthält (vgl. § 4). Die von den Veränderlichen unabhängigen Factoren werden hierbei vorläufig ausser Acht gelassen, da sie erst mit der Betrachtung der *ganzen* Functionen von $\mathfrak{R}'$, $\mathfrak{R}''$, $\mathfrak{R}'''$, ..., d. h. der *ganzen* Grössen des Bereichs zu fixiren sind.

§ 2.

Die algebraischen Grössen; ihre Eintheilung in Gattungen.

Jede Wurzel einer irreductibeln Gleichung n^{ten} Grades, deren Coefficienten dem Rationalitäts-Bereich $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$ angehören, heisst eine

algebraische Function n^{ter} Ordnung der Grössen $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots$. Die n Wurzeln einer und derselben Gleichung sind „conjugirte algebraische Functionen“ von $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots$.

Wenn man eine bestimmte algebraische Function n^{ter} Ordnung von $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots$ zu eben diesen Grössen $\mathfrak{R}$ hinzunimmt oder „adjungirt“, so constituirt die Gesammtheit derjenigen dem neuen Rationalitäts-Bereich angehörigen Grössen, welche algebraische Functionen n^{ter} Ordnung sind, eine bestimmte *„Gattung“ (genus)* algebraischer Functionen n^{ter} Ordnung von $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots$, also eine besondere, dem Bereich $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$ *„entstammende“* Grössengattung. Die Zahl n soll auch die *„Ordnung der Gattung“* bezeichnen. Sind $\mathfrak{G}, \mathfrak{G}'$ zwei algebraische Functionen verschiedener Gattungen von der Beschaffenheit, dass sämmtliche Functionen der Gattung $\mathfrak{G}$ zum Rationalitäts-Bereich $(\mathfrak{G}', \mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$ gehören, so soll die Beziehung der beiden Gattungen dadurch zum Ausdruck gebracht werden, dass die Gattung $\mathfrak{G}$ als unter der Gattung $\mathfrak{G}'$ *„enthalten“* bezeichnet wird. — Die Ordnung der enthaltenen Gattung $\mathfrak{G}$ ist ein Divisor der Ordnung der enthaltenden Gattung $\mathfrak{G}'$. Denn wenn $f(x)$ eine rationale Function von x bedeutet und mit $x_1, x_2, \ldots x_n$ die n conjugirten algebraischen Functionen x bezeichnet werden, so muss *jeder* irreductible Factor des Products

$$\Pi(y - f(x_k)) \qquad (k = 1, 2, \ldots n)$$

offenbar für *jeden* der conjugirten Werthe $y = f(x_k)$ verschwinden, und diese irreductibeln Factoren müssen also sämmtlich identisch sein. Die Anzahl der unter einander *verschiedenen* Werthe $f(x_k)$, d. h. die Ordnung der algebraischen Function $f(x)$, ist demnach ein Theiler von n (vgl. meinen citirten Aufsatz vom März 1879). — Wenn conjugirte algebraische Functionen zu verschiedenen Gattungen gehören, so werden diese Gattungen selbst als *„conjugirt“* bezeichnet. Es giebt also höchstens so viel einander conjugirte Gattungen, als ihre Ordnung beträgt. Wenn die Anzahl nur *Eins* ist, d. h. also, wenn die Gattung keine conjugirten hat, so ist sie eine *„Galois*sche Gattung“.

Der Rationalitäts-Bereich $(\mathfrak{G}', \mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$ umfasst ausser den algebraischen Functionen der Gattung $\mathfrak{G}'$ noch alle diejenigen, welche den unter $\mathfrak{G}'$ enthaltenen Gattungen angehören, und dazu sind auch die rationalen Functionen von $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots$ zu rechnen, da sie gewissermassen die Gattung erster Ordnung bilden. Der bezeichnete Bereich soll *„der Bereich der Gattung $\mathfrak{G}'$“* genannt werden, und es wird also durch den Zusatz

des Wortes „Bereich" dem Gattungsbegriff eine erweiterte Bedeutung beigelegt. Die Gesammtheit der algebraischen Functionen höchster Ordnung, welche in dem Gattungs*bereich* enthalten sind, bildet die Gattung selbst, im engeren Sinne des Wortes. Das Verhältniss der Gattungen zu dem Bereich $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$, aus welchem sie entstammen, kann füglich dadurch zum Ausdruck kommen, dass dieser als der *„Stammbereich"* der daraus hervorgegangenen Gattungen bezeichnet wird. Jeder Gattungsbereich enthält seinen Stammbereich.

Sind $\mathfrak{G}', \mathfrak{G}'', \mathfrak{G}''', \ldots$ beliebige Gattungen algebraischer Functionen von $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots$, so bildet die Gesammtheit der Grössen des Rationalitäts-Bereichs $(\mathfrak{G}', \mathfrak{G}'', \mathfrak{G}''', \ldots \mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$ wiederum einen Gattungsbereich $(\mathfrak{G}, \mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$, wie in dem zweiten Absatze des folgenden Paragraphen näher dargelegt wird. Die bestimmende Gattung $\mathfrak{G}$ ist hierbei ebensowohl dadurch charakterisirt, dass sie durch die algebraischen Functionen höchster Ordnung des Bereichs $(\mathfrak{G}', \mathfrak{G}'', \mathfrak{G}''', \ldots \mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$ gebildet wird, als dadurch, dass sie die Gattung niedrigster Ordnung ist, unter welcher die sämmtlichen Gattungen $\mathfrak{G}', \mathfrak{G}'', \mathfrak{G}''', \ldots$ enthalten sind.

§ 3.

Die natürlichen Rationalitäts-Bereiche und die Gattungs-Bereiche.

Die Wahl der Grössen $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots$, d. h. also der Elemente eines Rationalitäts-Bereichs, unterliegt an sich keinerlei Beschränkung, doch ist es für die Behandlung der algebraischen Grössen völlig bedeutungslos, transcendente Zahlengrössen oder transcendente Functionen von Variabeln unter die Elemente mit aufzunehmen; denn die Resultate bleiben ungeändert, wenn an Stelle solcher transcendenten neue unabhängige Veränderliche gesetzt werden. Sind nämlich die Resultate der Theorie algebraischer Functionen von $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots$ erst für diesen Fall, wo die transcendenten $\mathfrak{R}$ durch unabhängige Variable ersetzt sind, entwickelt, so können dieselben, ihrer Natur und Herleitung nach, nur durch solche Specialisation von Grössen $\mathfrak{R}$ alterirt oder modificirt werden, bei welcher *algebraische* Beziehungen zwischen denselben eintreten*). Es kann daher, unbeschadet der Allge-

*) In dem oben erwähnten, unvollendeten Aufsatze *Abels* (Oeuvres complètes 1839 Tome II p. 185) kommen Stellen vor, z. B. auf S. 188 und S. 196, aus welchen hervorzugehen scheint, dass *Abel* bei seiner ersten Beschäftigung mit dem Gegenstande noch glaubte, den Fall transcendenter Grössen $\mathfrak{R}$ mit in Betracht ziehen zu müssen.

meinheit, angenommen werden, ***dass die Elemente eines Rationalitäts-Bereichs nur aus einer Anzahl veränderlicher oder unbestimmter Grössen und algebraischer Functionen derselben bestehen.***

Es ist an sich klar, dass man zu den Elementen eines Rationalitäts-Bereichs, ohne denselben zu ändern, jede beliebige rationale Function derselben hinzufügen, sowie auch andererseits jede der Grössen $\mathfrak{R}$, welche eine rationale Function der übrigen ist, weglassen kann. Wenn ferner eine der Grössen $\mathfrak{R}$ eine ***algebraische*** Function der übrigen ist, so kann eine beliebige andere Function derselben Gattung dafür gesetzt werden. Da nun für zwei algebraische Functionen verschiedener Gattungen $\mathfrak{G}'$, $\mathfrak{G}''$ stets auf unendlich viele Weisen lineare Functionen mit ganzzahligen Coefficienten $\mathfrak{N}'\mathfrak{G}'+\mathfrak{N}''\mathfrak{G}''$ bestimmt werden können, welche die Gattung niedrigster Ordnung repräsentiren, unter denen beide Gattungen enthalten sind, so kann, wenn $\mathfrak{G}'$ und $\mathfrak{G}''$ unter den Elementen vorkommen, erst $\mathfrak{N}'\mathfrak{G}'+\mathfrak{N}''\mathfrak{G}''$ hinzugefügt, alsdann aber sowohl $\mathfrak{G}'$ als $\mathfrak{G}''$ weggelassen werden, und man gelangt auf diese Weise allmählich zu dem am Schlusse des § 2 angegebenen Resultat, dass der Rationalitäts-Bereich $(\mathfrak{G}', \mathfrak{G}'', \mathfrak{G}''', \ldots \mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$ mit einem Rationalitäts-Bereich $(\mathfrak{G}, \mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$ identisch ist, in welchem $\mathfrak{G}$ als Gattung niedrigster Ordnung bestimmt ist, unter der die sämmtlichen Gattungen $\mathfrak{G}'$, $\mathfrak{G}''$, $\mathfrak{G}'''$, ... enthalten sind. Man kann sich hiernach schliesslich auf die Annahme solcher Rationalitäts-Bereiche $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$ beschränken, in welchen die Elemente eine Anzahl veränderlicher oder unbestimmter Grössen sind, zu denen höchstens ***eine*** algebraische Function derselben tritt. Für ein solches Hinzutreten von Grössen $\mathfrak{R}$, die den Rationalitäts-Bereich in einer für die algebraische Betrachtung wesentlichen Weise modificiren, bedient man sich seit ***Galois*** des technischen Ausdrucks der Adjunction. Die allgemeinste Annahme kann also dahin formulirt werden, dass für die Grössen $\mathfrak{R}$ eine Anzahl Variabler zu setzen und denselben höchstens ***eine*** algebraische Function zu adjungiren ist. Hierin ist auch der Fall mit inbegriffen, wo die Grössen $\mathfrak{R}$ überhaupt fehlen, d. h. der Fall, in welchem der Rationalitäts-Bereich derjenige der rationalen Zahlen, also der ***„absolute“*** Rationalitäts-Bereich ist, und dieser kann offenbar auch dadurch bezeichnet werden, dass nur ***eine*** Grösse $\mathfrak{R}$ und diese gleich ***Eins*** angenommen wird. Die algebraischen Functionen der Grössen $\mathfrak{R}$, d. h. die aus dem Rationalitäts-Bereich hervorgehenden algebraischen Grössen sind in diesem Falle ***„algebraische Zahlen“;*** sie sind es offenbar auch in dem Falle, wenn nur ***ein*** Element

$\mathfrak{R}$, und dieses selbst gleich einer bestimmten algebraischen Zahl angenommen wird.

Wenn für den allgemeinen Fall, wo die Elemente $\mathfrak{R}$ eine Anzahl veränderlicher oder unbestimmter Grössen enthalten, unbedenklich von algebraischen Functionen der Grössen $\mathfrak{R}$ die Rede sein konnte, so erscheint doch diese Ausdrucksweise nicht mehr völlig zutreffend, wenn nur *eine* Grösse $\mathfrak{R} = 1$ vorhanden ist. Um diesen besonderen Fall auch in der *Ausdrucksweise* mit zu umfassen, ist es vorzuziehen, die algebraischen Functionen der Grössen $\mathfrak{R}$ auch im allgemeinen Falle veränderlicher oder unbestimmter Grössen $\mathfrak{R}$ als algebraische, dem Rationalitäts-Bereich $(\mathfrak{R})$ entstammende *Grössen* zu bezeichnen. Da jedoch die Anwendung des Begriffs der algebraischen Functionen auf den besonderen Fall $\mathfrak{R} = 1$ nur in ganz äusserlicher Hinsicht bedenklich erscheint, so kann dieser Begriff und die dem entsprechende Ausdrucksweise neben der anderen, welche sich dem Falle $\mathfrak{R} = 1$ besser anpasst, gebraucht werden.

Ein Rationalitäts-Bereich ist im Allgemeinen ein *willkürlich* abgegrenzter Grössenbereich, doch nur, so weit es der Begriff gestattet. Da nämlich ein Rationalitäts-Bereich nur durch Hinzufügung beliebig gewählter Elemente $\mathfrak{R}$ vergrössert werden kann, so erfordert jede willkürliche Ausdehnung seiner Begrenzung zugleich die Umschliessung *aller* durch das neue Element rational ausdrückbaren Grössen. Es giebt aber auch *natürlich* abgegrenzte Rationalitäts-Bereiche, so das Reich der gewöhnlichen rationalen Zahlen, welches als das absolute in allen Rationalitäts-Bereichen enthalten ist und, wie es durch $\mathfrak{R} = 1$ bezeichnet worden, auch gewissermassen die absolute Einheit des Rationalitäts-Begriffs repräsentirt. Auch das Reich der rationalen Functionen von $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots$, wenn diese sämmtlich unabhängige Variable bedeuten, ist ein *„natürlich“* abgegrenztes; es ist darin das Reich der rationalen Zahlen sowie überhaupt das der rationalen Functionen von einem *Theile* der Variabeln $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots$ mit enthalten.

Aus einem Rationalitäts-Bereich „gehen die verschiedenen Gattungen algebraischer Functionen hervor“; sie können wieder ganz oder theilweise in einen grösseren Bereich zusammengefasst werden, in welchem dann nothwendig der ursprüngliche Rationalitäts-Bereich enthalten ist. Es ist an sich klar, dass, wenn die Elemente $\mathfrak{R}_0', \mathfrak{R}_0'', \ldots$ zu einem Rationalitäts-Bereich $(\mathfrak{R}', \mathfrak{R}'', \ldots)$ gehören, der Rationalitäts-Bereich $(\mathfrak{R}_0', \mathfrak{R}_0'', \ldots)$ ein Theilbereich dessen mit den Elementen $\mathfrak{R}', \mathfrak{R}'', \ldots$ ist. Sind die Elemente $\mathfrak{R}_0', \mathfrak{R}_0'', \ldots$

und $\mathfrak{R}', \mathfrak{R}'', \ldots$ *gegenseitig* durch einander rational ausdrückbar, so sind die beiden dadurch bestimmten Rationalitäts-Bereiche identisch.

Die *sämmtlichen* aus einem natürlichen Rationalitäts-Bereich hervorgehenden Gattungen algebraischer Grössen bilden zusammen ein geschlossenes, den Stammbereich mit einschliessendes Grössenreich, so z. B. das Gesammtreich der algebraischen Zahlen, oder das Gesammtreich aller algebraischen Functionen von unabhängigen Variabeln $\mathfrak{R}', \mathfrak{R}'', \ldots,$ welches das erstere in sich schliesst. Man kann aber auch ein solches kleineres *Gesammt*reich $(\mathfrak{R}'_0, \mathfrak{R}''_0, \ldots)$ einem grösseren Rationalitäts-Bereich $(\mathfrak{R}'_0, \mathfrak{R}''_0, \ldots, \mathfrak{R}', \mathfrak{R}'', \ldots)$ anschliessen und also z. B. im Falle $\mathfrak{R}_0 = 1$ einen aus variabeln Elementen $\mathfrak{R}$ gebildeten Rationalitäts-Bereich $(\mathfrak{R}', \mathfrak{R}'', \ldots)$ mit dem Reiche aller algebraischen Zahlen verbinden, d. h. also bei der Behandlung algebraischer Functionen der Variabeln $\mathfrak{R}', \mathfrak{R}'', \ldots$ von den „Constanten" absehen. Dies geschieht z. B. in der Regel bei analytisch-geometrischen Untersuchungen, wenn $\mathfrak{R}', \mathfrak{R}'', \ldots$ die Coordinaten bedeuten. So kommt es bei der Frage nach der Zerlegbarkeit einer ganzen rationalen Function $F(x, y, z)$, wenn man $F(x, y, z) = 0$ als die Gleichung einer algebraischen Fläche betrachtet, in der Regel nicht darauf an, ob die Coefficienten der Factoren rationale Zahlen sind oder nicht. Aber man braucht, wie dieses Beispiel zeigt, bei bestimmten Fragen doch nur die Adjunction *bestimmter* Grössen, und anstatt von vorn herein unendlich viele Grössen zu adjungiren, genügt es daher, sich nur die Adjunction besonderer, aus der Untersuchung selbst sich ergebender Grössen vorzubehalten. — Im Allgemeinen hat sich also, wie oben dargelegt worden, die arithmetische Behandlung der algebraischen Grössen auf Rationalitäts-Bereiche mit lauter unabhängigen Variabeln und solche, bei denen überdies noch eine Gattung algebraischer Functionen derselben adjungirt ist, also auf *„natürliche Stammbereiche und Gattungsbereiche"* zu beschränken (vgl. meinen Aufsatz „Ueber die verschiedenen *Sturm*schen Reihen" im Monatsbericht der Berliner Akademie vom Febr. 1873, S. 122 und 123).

§ 4.

Die Zerlegung ganzer Functionen von Variabeln in irreductible Factoren.

Die im Art. 1 aufgestellte Definition der Irreductibilität entbehrt so lange einer sicheren Grundlage, als nicht eine Methode angegeben ist, mittels deren bei einer bestimmten, vorgelegten Function entschieden werden

kann, ob dieselbe der aufgestellten Definition gemäss irreductibel ist oder nicht*). Die zunächst sich darbietende Methode, die Coefficienten der Theiler einer ganzen Function von Veränderlichen durch Elimination aus den dafür bestehenden Gleichungen zu bestimmen, empfiehlt sich schon um desswillen nicht, weil bei naturgemässer und vollständiger Entwickelung der Theorie der Elimination die Zerlegung ganzer Functionen in ihre Factoren gebraucht wird. Desshalb soll hier eine neue Methode dargelegt werden, welche nur einfache, hier bereits verwendbare Hülfsmittel in Anspruch nimmt.

Ist erstens zu entscheiden, ob eine ganze ganzzahlige Function einer Variabeln x rationale Divisoren hat oder nicht, so braucht man, wenn dieselbe vom Grade $2n$ oder $2n+1$ ist, offenbar nur die etwaigen Theiler n^{ten} oder niedrigeren Grades zu ermitteln. Sind nun $r_0, r_1, r_2, \ldots r_n$ beliebige, von einander verschiedene, positive oder negative ganze Zahlen, und setzt man

$$g_0(x) = \frac{(x-r_1)(x-r_2)\ldots(x-r_n)}{(r_0-r_1)(r_0-r_2)\ldots(r_0-r_n)}, \quad g_1(x) = \frac{(x-r_0)(x-r_2)\ldots(x-r_n)}{(r_1-r_0)(r_1-r_2)\ldots(r_1-r_n)}, \quad \ldots,$$

so ist jede ganze ganzzahlige Function $f(x)$, deren Grad höchstens gleich n ist, als ganze ganzzahlige lineare Function der $n+1$ Functionen $g(x)$ darstellbar, und zwar ist

$$f(x) = f(r_0)g_0(x) + f(r_1)g_1(x) + \cdots + f(r_n)g_n(x).$$

Soll also $f(x)$ ein Theiler der vorgelegten Function $F(x)$ sein, so muss bei dieser Darstellungsweise der Coefficient von $g_h(x)$ ein Divisor der ganzen Zahl $F(r_h)$ sein, und man hat daher nur eine endliche Anzahl von Coefficienten-Systemen zu discutiren, um alle Theiler von $F(x)$ zu erhalten oder der Irreductibilität von $F(x)$ gewiss zu sein. — Eben dasselbe Verfahren kann nun direct auf ganze Functionen mehrerer Variabeln ausgedehnt oder beim allmählichen Uebergange zu 2, 3 und mehr Variabeln angewendet werden. Aber es ist schon an sich (theoretisch) auch für Functionen mehrerer Variabeln vollkommen ausreichend, da eine ganze Function von $x, x', x'', x''', \ldots x^{(n)}$, wenn

$$x' = c_1 x^g, \quad x'' = c_2 x^{g^2}, \quad x''' = c_3 x^{g^3}, \quad \ldots \quad x^{(n)} = c_n x^{g^n}$$

gesetzt und g hinreichend gross genommen wird, in eine ganze Function

*) Das analoge Bedürfniss, welches freilich häufig unbeachtet geblieben ist, zeigt sich auch in vielen anderen Fällen, bei Definitionen wie bei Beweisführungen, und ich werde bei einer anderen Gelegenheit in allgemeiner und eingehender Weise darauf zurückkommen.

der einzigen Variabeln x übergeht, welche in Beziehung auf ihre Zerlegbarkeit so wie überhaupt in algebraischer Hinsicht die transformirte Function von $x, x', x'', \dots x^{(n)}$ durchaus zu ersetzen geeignet ist. Bei genügender Grösse der Zahl g werden nämlich die verschiedenen Producte von Potenzen der $n+1$ Variabeln x in ganze Functionen der einzigen Variabeln x verwandelt, welche von lauter verschiedenen Graden und also linear unabhängig sind. (Vgl. meine Mittheilung im Monatsbericht der Berliner Akademie vom Nov. 1880, S. 938, 939.)

Nachdem hiermit eine Methode angegeben worden, mittels deren eine ganze ganzzahlige Function von beliebig vielen Veränderlichen in ihre irreductibeln Factoren zerlegt werden kann, wenn für den Begriff der Irreductibilität der natürliche Rationalitäts-Bereich festgehalten wird, bleibt nur noch übrig, die Zerlegung auch für den Fall, wo eine der Grössen $\mathfrak{R}$ eine algebraische Grösse ist, zu bewirken. Dies geschieht in folgender Weise, wenn der Einfachheit halber eine der Variabeln hervorgehoben wird und also nur die Zerlegung einer ganzen Function $F(x)$ zu bewirken ist, deren Coefficienten einem Rationalitäts-Bereich $(\mathfrak{R}, \mathfrak{R}', \mathfrak{R}'', \dots)$ angehören, in welchem $\mathfrak{R}$ eine algebraische Function der übrigen Grössen $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \dots$ ist. Dabei kann angenommen werden, dass die Function $F(x)$ keine gleichen Factoren enthält; denn anderenfalls würde man dieselbe von gleichen Factoren dadurch befreien können, dass man sie durch den grössten Theiler, den die Function $F(x)$ mit ihrer Ableitung gemein hat, dividirt. Man setze nun zuvörderst $z+u\mathfrak{R}$ an Stelle von x in $F(x)$, wo u eine unbestimmte Grösse bedeutet; man betrachte ferner F selbst als Function von x und der zum Rationalitäts-Bereich gehörigen algebraischen Grösse $\mathfrak{R}$, welche also auch in den Coefficienten vorkommen kann, bezeichne demnach die Function F durch $F(x, \mathfrak{R})$ und bilde das Product aller mit einander conjugirten Ausdrücke

$$F(z+u\mathfrak{R}, \mathfrak{R}),$$

d. h. aller derjenigen, welche entstehen, wenn man die mit $\mathfrak{R}$ conjugirten algebraischen Grössen an Stelle von $\mathfrak{R}$ setzt. Dieses Product ist eine ganze Function von x, deren Coefficienten rationale Functionen der Variabeln $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \dots$ sind, kann also nach dem Vorhergehenden in irreductible Factoren zerlegt werden. Sind diese Factoren: $F_1(z), F_2(z), \dots$, so bilden, wie leicht zu sehen, die grössten gemeinschaftlichen Theiler von

$$F(z+u\mathfrak{R}, \mathfrak{R}) \quad \text{und} \quad F_k(x)$$

für $h = 1, 2, \ldots$ die irreductibeln Factoren von $F(z + u\mathfrak{R}, \mathfrak{R})$, aus denen die Factoren von $F(x)$ selbst unmittelbar hervorgehen, wenn wieder $x - u\mathfrak{R}$ an Stelle von z gesetzt wird. Es ist noch zu bemerken, dass die Einführung von $z + u\mathfrak{R}$ an Stelle von x zu dem Zwecke erfolgt ist, das Vorkommen von $\mathfrak{R}$ in den Coefficienten zu sichern.

Für jede ganze Function beliebig vieler Veränderlicher, deren Coefficienten einem festgesetzten Rationalitäts-Bereich $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$ angehören, ist hiermit die Möglichkeit ihrer Zerlegung in irreductible Factoren dargethan. Dass eine solche Zerlegung nur in einer einzigen Weise möglich, also vollkommen bestimmt ist, beruht — da man sich aus dem oben angeführten Grunde auf Functionen einer Variabeln beschränken kann — einfach auf dem Satze, dass ein Product von zwei ganzen Functionen von x nur dann durch einen irreductibeln Factor theilbar sein kann, wenn eine der beiden Functionen diesen Factor enthält. Für den absoluten Rationalitäts-Bereich behält dieser Satz auch noch seine Geltung, wenn der irreductible Factor eine Function *null*ten Grades ist, also x gar nicht enthält. Ein solcher irreductibler Factor ist demnach eine gewöhnliche Primzahl, und es ist schon in Art. 42 von *Gauss'* Disqq. Arithm. nachgewiesen, dass ein Product $\varphi(x)\psi(x)$ nicht durch eine Primzahl p theilbar sein kann, ohne dass einer der Factoren $\varphi(x)$ oder $\psi(x)$ durch p theilbar ist. In dem angenommenen Falle $\mathfrak{R} = 1$ sind die Functionen, deren Zerlegung entwickelt worden ist, ***ganze ganzzahlige Functionen beliebig vieler Veränderlicher,*** und die obigen Ausführungen enthalten daher die Methode, wie jede solche Function in irreductible Factoren zerlegt werden kann, und zugleich den Nachweis, dass dies nur auf eine einzige völlig bestimmte Weise möglich ist.

§ 5.

Die ganzen algebraischen Grössen; ihre Eintheilung in Arten.

Wenn der Rationalitäts-Bereich $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$ ein natürlicher ist, d. h. wenn es der Bereich $\mathfrak{R} = 1$ ist, oder wenn die Elemente $\mathfrak{R}$ sämmtlich unabhängige Variable sind, so bilden die ganzen ganzzahligen Functionen von $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots$ einen in sofern wieder in sich geschlossenen Theilbereich, als die sämmtlichen ganzen ganzzahligen Functionen der darin enthaltenen Grössen ebenfalls mit darin enthalten sind. Diese ganzen Functionen von $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots$ sollen kurzweg als die *„ganzen"* Grössen des

Rationalitäts-Bereichs bezeichnet werden. Für den dieselben umfassenden Theilbereich könnte auch füglich, nach Analogie des Ausdrucks „Rationalitäts-Bereich“, die Benennung „*Integritäts-Bereich*“ eingeführt werden. Doch werde ich in der vorliegenden Arbeit von dieser Benennung kaum Gebrauch machen, sondern nur die Bezeichnung des Theilbereichs der „*ganzen*“ Grössen eines Rationalitäts-Bereichs mit den Elementen $\mathfrak{R}'$, $\mathfrak{R}''$, $\mathfrak{R}'''$, ... durch eckige Parenthesen anwenden und denselben demgemäss als den Bereich $[\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots]$ von dem gesammten Rationalitäts-Bereich $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$ unterscheiden. Dies vorausgeschickt, kann die Definition der *ganzen algebraischen* Functionen in einfacher Form gegeben werden.

Eine Grösse x soll eine „*ganze algebraische Function der Variabeln* $\mathfrak{R}$“ oder eine „*ganze algebraische Grösse*“ genannt werden, wenn sie einer Gleichung genügt, in welcher der Coefficient der höchsten Potenz von x gleich *Eins* ist, und die übrigen Coefficienten ganze ganzzahlige Functionen der Variabeln $\mathfrak{R}$, also Grössen des Bereichs $[\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots]$ sind. Für den Fall $\mathfrak{R} = 1$ sollen die ganzen algebraischen Grössen auch als „*ganze algebraische Zahlen*“ bezeichnet werden. Für den Fall veränderlicher $\mathfrak{R}$ ist eine Grösse als ganze algebraische Function einer der Variabeln $\mathfrak{R}$ dadurch charakterisirt, dass sie für endliche Werthe derselben niemals unendlich wird. Da ganze algebraische Functionen von ganzen algebraischen Grössen offenbar selbst ganze algebraische Grössen sind, so bildet die Gesammtheit der aus einem natürlichen Stammbereich $[\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots]$ hervorgehenden ganzen algebraischen Grössen ein in sich geschlossenes algebraisches Grössenreich.

Für jeden natürlichen Rationalitäts-Bereich $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$ gilt der Satz, dass eine ganze algebraische Grösse, wenn sie rational ist, auch eine ganze ganzzahlige Function von $\mathfrak{R}'$, $\mathfrak{R}''$, $\mathfrak{R}'''$, ... sein muss. Soll nämlich eine gebrochene rationale Function von $\mathfrak{R}'$, $\mathfrak{R}''$, $\mathfrak{R}'''$, ... einer Gleichung n^{ten} Grades genügen, in welcher der Coefficient von x^n gleich *Eins* ist, und die übrigen Coefficienten ganze ganzzahlige Functionen von $\mathfrak{R}'$, $\mathfrak{R}''$, $\mathfrak{R}'''$, ... sind, so muss offenbar die n^{te} Potenz des Zählers der gebrochenen rationalen Functionen durch den Nenner theilbar sein. Dies ist aber, da Zähler und Nenner nach § 4 in ihre irreductibeln Factoren zerlegt vorausgesetzt werden können, unmöglich, wenn nicht der Nenner gleich *Eins* ist. Falls eine der Grössen $\mathfrak{R}$ eine algebraische Function der übrigen und also der Rationalitäts-Bereich ein Gattungsbereich ist, hat der Satz — genau in der obigen

Form — nicht mehr unbeschränkte Geltung; so ist z. B. für $\mathfrak{R} = \sqrt{-3}$ die dritte Wurzel der Einheit $\frac{1}{2}(-1+\sqrt{-3})$, obgleich in Bruchform erscheinend, algebraisch ganz.

Bezeichnet $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$, wie durchweg in diesem und dem folgenden Paragraphen, einen natürlichen Rationalitäts-Bereich, und sind $\mathfrak{S}'$, $\mathfrak{S}''$, $\mathfrak{S}'''$, ... irgend welche jenem Bereich entstammende, *ganze* algebraische Grössen der Gattung $\mathfrak{G}$, so bilden diejenigen ganzen ganzzahligen Functionen von

$$\mathfrak{R}', \quad \mathfrak{R}'', \quad \mathfrak{R}''', \quad \ldots; \quad \mathfrak{S}', \quad \mathfrak{S}'', \quad \mathfrak{S}''', \quad \ldots,$$

welche der Gattung angehören, eine besondere *„Art"* oder *„Species"* derselben. Ebenso wie der Begriff der Gattung in § 2 durch den des Gattungsbereichs erweitert worden ist, soll auch der Begriff der Art erweitert und im *„Art-Bereich"* $[\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots; \mathfrak{S}', \mathfrak{S}'', \mathfrak{S}''', \ldots]$ die *Gesammtheit* der ganzen ganzzahligen Functionen der „Elemente" $\mathfrak{R}$ und $\mathfrak{S}$ zusammengefasst werden. Der Art-Bereich schliesst also auch ganze algebraische Grössen von Gattungen, die nicht zur Gattung $\mathfrak{G}$ gehören, sondern nur unter derselben enthalten sind, in sich ein, aber er ist vollständig in dem Gattungs*bereich* $(\mathfrak{G})$ enthalten, bildet also einen Theilbereich desselben. Auch verschiedene Arten einer und derselben Gattung stehen, wie die Gattungen selbst, in der Beziehung zu einander, dass eine unter der anderen enthalten, dass also ein Art-Bereich von dem anderen eingeschlossen ist. Die sämmtlichen Bereiche der besonderen Arten einer Gattung sind, wie sich von selbst versteht, in dem Gesammtbereich der ganzen algebraischen Grössen der Gattung enthalten. Dass aber auch dieser Gesammtbereich selber ein „Art-Bereich" im oben definirten Sinne des Wortes ist, d. h. also, dass ganze algebraische Grössen $\mathfrak{S}'$, $\mathfrak{S}''$, $\mathfrak{S}'''$, ... existiren, durch welche im Verein mit den Grössen $\mathfrak{R}$ sich alle ganzen algebraischen Grössen der Gattung ganz und rational darstellen lassen, bedarf eines besonderen Beweises; es ist dies eines der Fundamente der arithmetischen Theorie der algebraischen Grössen. Die durch solche Grössen $\mathfrak{S}$ bestimmte Art soll, um ihrem Verhältniss zu den übrigen Arten Ausdruck zu geben, als die *„Haupt-Art"* oder *„Haupt-Species"* bezeichnet werden.

Nach den gegebenen Begriffsbestimmungen enthalten die verschiedenen Arten algebraischer Grössen überhaupt *nur ganze* algebraische Grössen; dennoch soll zur Erinnerung in der Regel das Beiwort „ganz" hinzugefügt

werden. Es ist ferner hervorzuheben, dass die „Grössen der Haupt-Art" mit den „ganzen algebraischen Grössen der Gattung" identisch sind, und es soll nur, je nachdem auf den Gattungs- oder Art-Begriff mehr Gewicht zu legen ist, die eine oder die andere Ausdrucksweise vorgezogen werden.

Die Bezeichnung der hier unterschiedenen Kategorieen ganzer algebraischer Grössen als „Arten" oder „Species" ist *Dirichlet* entlehnt. Im zweiten Theile seiner berühmten Abhandlung „Recherches sur diverses applications de l'Analyse infinitésimale à la Théorie des Nombres" (Journal für Mathematik. Bd. 21 S. 2) hat er die von *Gauss* „eigentlich und uneigentlich primitiv" genannten quadratischen Formen als solche von erster und zweiter Art (formes de première et de seconde espèce) bezeichnet. Geht man von den quadratischen Formen zu den complexen Zahlen über, welche aus ihren Linearfactoren entstehen, so entsprechen den beiden *Dirichlet*schen „Arten" eben diejenigen, für welche oben diese Benennung eingeführt ist. Im Uebrigen aber sind es die verschiedenen „Ordnungen" der quadratischen Formen, denen die hier unterschiedenen „Arten" der zugehörigen complexen Zahlen entsprechen, und es erscheint mir als ein Vortheil, dass der *Gauss*sche Ausdruck „Ordnung", welcher schon so viele Bedeutungen hat, durch die in erweitertem Sinne gebrauchte *Dirichlet*sche Bezeichnung umgangen wird.

§ 6.

Lineare Darstellung der Grössen der Hauptart durch eine endliche Anzahl von Elementen.

Um den Nachweis zu führen, dass die Gesammtheit der ganzen algebraischen Grössen einer dem natürlichen Rationalitäts-Bereich $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$ entstammenden Gattung $\mathfrak{G}$ in der That, wie im vorigen Paragraphen gesagt ist, eine „Art" und zwar die „Hauptart" bildet, soll nunmehr gezeigt werden, dass sich jede ganze algebraische Grösse der Gattung $\mathfrak{G}$ als homogene ganze lineare Function einer endlichen Anzahl solcher Grössen mit Coefficienten aus dem Bereich $[\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots]$ darstellen lässt, d. h. so, dass die Coefficienten ganze ganzzahlige Functionen von $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots$ sind. Dabei stütze ich mich in erster Linie darauf, dass jede Grösse einer Gattung n^{ter} Ordnung als homogene ganze lineare Function von n linear unabhängigen Grössen der Gattung ausdrückbar ist, d. h. von n Grössen, zwischen denen keine lineare Relation mit rationalen, dem Bereich $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$ angehörigen Coefficienten besteht. Bei einer solchen Dar-

stellung brauchen aber die Coefficienten der homogenen linearen Function nicht nothwendig ganz zu sein, selbst dann nicht, wenn jede der n Grössen und auch die dargestellte Grösse ganz ist. Indessen tritt in diesem Falle offenbar nur die aus den n zur Darstellung verwendeten Grössen und ihren Conjugirten gebildete Determinante als Nenner der Coefficienten auf. Es lassen sich daher alle ganzen algebraischen Grössen der Gattung als homogene ganze lineare Functionen von n ganzen Grössen der Gattung so darstellen, dass die Coefficienten gebrochene Functionen von $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots$ mit einem bestimmten Nenner werden, welcher das Quadrat jener Determinante, also, als ganze symmetrische Function von conjugirten ganzen algebraischen Grössen, eine ganze Function von $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots$ ist und als *„die Discriminante der n Grössen“* bezeichnet werden soll. Da nun aber nicht *alle* linearen Functionen der n Grössen mit solchen Coefficienten *ganze* algebraische Grössen der Gattung sind, so handelt es sich nur noch darum, die Bedingungen für die Coefficienten festzustellen, unter denen die dargestellte Grösse algebraisch ganz wird. Hierbei genügt es offenbar, wie hier und im vorigen Paragraphen durchweg geschehen ist, nur natürliche Rationalitäts-Bereiche in Betracht zu ziehen, wo die Grössen $\mathfrak{R}$ lediglich unabhängige Veränderliche sind, also keine algebraische Grösse enthalten. In dem einfachsten Falle, wo die Anzahl dieser Veränderlichen gleich Null oder also $\mathfrak{R} = 1$ ist, reicht es hin, für die Coefficienten alle echten Brüche zu setzen, deren Nenner die Discriminante ist, und alle auf diese Weise resultirenden algebraischen Zahlen darauf hin zu prüfen, ob sie *ganz* sind oder nicht. Nimmt man alsdann diejenigen derselben, welche sich als algebraisch ganz erweisen, als neue Elemente zu den ursprünglichen n Elementen der Darstellung hinzu, so leuchtet ein, dass eine homogene lineare ganzzahlige Function aller dieser Elemente an sich eine ganze algebraische Zahl der Gattung ist und auch zur Darstellung *aller* ausreicht. — Für den Fall, wo die Grössen $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots$ Variable sind, ist die allgemeine Theorie der Elimination zu Hülfe zu nehmen (vgl. § 10). Sind z. B. nur zwei Veränderliche $\mathfrak{R}' = v$, $\mathfrak{R}'' = w$ vorhanden, so kann vorausgesetzt werden, dass die Zahl, welche den Grad der Discriminante in Beziehung auf v bezeichnet, zugleich die Dimension in Beziehung auf v und w angiebt, da sich dies durch lineare Transformation der beiden Variabeln stets erreichen lässt. Alsdann ist eine homogene lineare Function der n linear unabhängigen algebraischen Grössen, die zunächst als Elemente der Darstellung dienen,

zu bilden, deren Coefficienten als ganze Functionen von v, dividirt durch die Discriminante, anzunehmen sind, und zwar so, dass der Grad dieser ganzen Functionen kleiner als der Grad der Discriminante ist. Die Coefficienten dieser n ganzen Functionen von v sind nun als ganze Functionen von w so zu bestimmen, dass jene angenommene homogene lineare Function der n Elemente algebraisch ganz wird. Dadurch erhält man für die zu bestimmenden ganzen Functionen von w ein System von Bedingungsgleichungen, in welchem die Coefficienten ganze Functionen von w sind, und welches — wie aus der Entstehung erhellt — so beschaffen sein muss, dass, wenn zwei verschiedene Systeme von Functionen

$$\varphi_1(w), \quad \varphi_2(w), \quad \ldots; \quad \psi_1(w), \quad \psi_2(w), \quad \ldots$$

demselben genügen würden, auch deren lineare Verbindungen

$$\lambda\varphi_1(w)+\mu\psi_1(w), \quad \lambda\varphi_2(w)+\mu\psi_2(w), \quad \ldots$$

das Gleichungssystem befriedigen müssten. Man erschliesst hierdurch aus der Natur des Problems selbst, dass die Resolvente des Gleichungssystems (vgl. § 10) linear sein muss, und dass sich eine Anzahl der zu bestimmenden Functionen von w als lineare Functionen der übrigen in der Form

$$\varphi_1\theta_1+\varphi_2\theta_2+\cdots+\varphi_m\theta_m = \varphi_{m+1}\theta, \quad \varphi_1\theta'_1+\varphi_2\theta'_2+\cdots+\varphi_m\theta'_m = \varphi_{m+2}\theta, \quad \ldots$$

ergiebt, wenn $\varphi_1, \varphi_2, \ldots$ die zu bestimmenden, und $\theta, \theta_1, \theta_2, \ldots, \theta'_1, \theta'_2, \ldots$ bestimmte ganze Functionen von w bedeuten. Die Functionen $\varphi_1, \varphi_2, \ldots$ sind hiernach nur der Bedingung unterworfen, dass die Ausdrücke

$$\varphi_1\theta_1+\varphi_2\theta_2+\cdots+\varphi_m\theta_m, \quad \varphi_1\theta'_1+\varphi_2\theta'_2+\cdots+\varphi_m\theta'_m, \quad \ldots$$

sämmtlich durch θ theilbar sein sollen, und daraus resultiren, wenn die Functionen φ sämmtlich von niedrigerem Grade als θ angenommen werden, lineare Gleichungen für die Coefficienten der m Functionen $\varphi_1, \varphi_2, \ldots \varphi_m$. Bei dieser Methode zur Bestimmung einer allgemeinen Form der ganzen algebraischen Grössen einer Gattung ist der Einfachheit halber von den Zahlcoefficienten abgesehen und nur dafür gesorgt worden, dass die dargestellte Grösse in Beziehung auf die Variabeln v und w ganz, d. h. also für endliche Werthe derselben niemals unendlich werde. Die Methode selbst ist aber auch anzuwenden, um aus jener allgemeinen Form diejenige speciellere zu ermitteln, welche nur ganze algebraische Grössen, im vollen Sinne des Wortes, enthält; sie führt ganz unmittelbar zu einer Reihe von solchen Grössen, welche als Elemente zur Darstellung aller ganzen algebraischen

Grössen der Gattung in der oben bezeichneten Weise dienen können, nämlich so, dass eine homogene ganze lineare Function der Elemente mit Coefficienten, die ganze rationale Functionen von v und w sind, jede ganze algebraische der Gattung angehörige Function von v und w repräsentirt.

§ 7.

Besondere Fälle, in denen die lineare Darstellung der Grössen der Art nur eine der Ordnungszahl gleiche Anzahl von Elementen erfordert.

In besonderen Fällen genügen zur Darstellung der sämmtlichen Grössen einer bestimmten Art solche Systeme von Elementen, deren Anzahl die Ordnung der Gattung nicht übersteigt. Dies findet namentlich durchweg für den Bereich $\mathfrak{R} = 1$ und auch für den Fall einer einzigen Variabeln $\mathfrak{R}$ statt, sofern alsdann von den Zahlcoefficienten abgesehen wird; es findet ferner unter derselben Bedingung — es bleibe dahin gestellt, ob die Bedingung *nothwendig* ist — im Bereich von n unabhängigen Variabeln $(\mathfrak{R}', \mathfrak{R}'', \dots \mathfrak{R}^{(n)})$ für alle Gattungen statt, die durch irgend eine rationale Function der n Wurzeln der Gleichung

$$x^n + \mathfrak{R}' x^{n-1} + \mathfrak{R}'' x^{n-2} + \cdots + \mathfrak{R}^{(n)} = 0$$

repräsentirt werden (vgl. § 12). Um ein zur Reduction der Anzahl der Elemente dienendes Verfahren darzulegen, wähle ich den Fall, wo nur eine Variable $\mathfrak{R} = v$ vorhanden ist. Bedeutet n die Ordnung der Gattung, und bilden die $n+m$ ganzen algebraischen Grössen $x', x'', \dots x^{(n+m)}$ ein zur Darstellung aller ganzen algebraischen Grössen der Species ausreichendes System von Elementen, so kann man sich diese so geordnet denken, dass die Discriminante der *ersten* n Grössen von möglichst niedrigem Grade, d. h. dass jede der übrigen Discriminanten von höherem oder gleich hohem Grade in v ist. Die m letzten Elemente lassen sich nun als homogene lineare Functionen der n ersten darstellen, und zwar so, dass die Coefficienten gebrochene rationale Functionen von v werden, deren Nenner jene Discriminante der ersten n Elemente oder ein Theiler derselben ist. Durch Hinzufügung homogener linearer Functionen von $x', x'', \dots x^{(n)}$, deren Coefficienten *ganze* Functionen von v sind, können daher die folgenden Elemente x so modificirt werden, dass bei ihrer Darstellung durch $x', x'', \dots x^{(n)}$ die Zähler der Coefficienten von niedrigerem Grade sind als die bezüglichen Nenner, und dass *ganze* Functionen von v als Coefficienten gar nicht vorkommen.

Nach dieser Modification, durch welche die Zahl der Elemente und auch der Grad der Discriminanten sich vermindert haben kann, sind die Elemente, also die n ersten nebst denjenigen von den m letzten, welche geblieben sind, zusammen von Neuem in der angegebenen Weise zu ordnen. Wird hierauf das obige Verfahren auf das neue Elementen-System und alsdann wiederholt angewendet, so muss einmal der Fall eintreten, dass die ersten n Elemente — weil ihre Discriminante schon von möglichst niedrigem Grade ist — an ihrer ersten Stelle verbleiben. In diesem Falle können keine weiteren Elemente mehr vorkommen; denn ein solches Element $x^{(n+1)}$ müsste bei der Darstellung durch die ersten n Elemente wenigstens *einen* Coefficienten haben, dessen Grad in Bezug auf v negativ wäre, und wenn dies der Coefficient von x' ist, so würde die Discriminante der n Elemente x'', x''', ... $x^{(n+1)}$ von niedrigerem Grade sein als die der Elemente $x', x'', \dots x^{(n)}$. Ich bemerke noch, dass genau dieselbe Deduction für den Fall $\mathfrak{R} = 1$ mit der Massgabe anwendbar ist, dass an Stelle der Grösse des Grades in Bezug auf v die Grösse der Zahlen selbst tritt (vgl. § 24).

§ 8.

Die Discriminanten der Gattungen und Arten.

Ein System von ganzen algebraischen Grössen $x', x'', \dots x^{(n+m)}$, einer bestimmten Art oder Species, welches so beschaffen ist, dass sich alle Grössen derselben in der Form

$$\varphi' x' + \varphi'' x'' + \cdots + \varphi^{(n+m)} x^{(n+m)}$$

darstellen lassen, wo $\varphi', \varphi'', \dots \varphi^{(n+m)}$ ganze ganzzahlige Functionen von $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \dots$ bedeuten, soll als ein „Fundamentalsystem der Art" und wenn es die Haupt-Art ist, auch als ein „Fundamentalsystem *der Gattung*" bezeichnet werden.

Damit auch für einen *Gattungs*-Bereich $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \dots)$ die in § 5 aufgestellte Begriffsbestimmung einer „ganzen algebraischen Grösse" oder einer „ganzen algebraischen Function der Elemente $\mathfrak{R}$" Geltung behalte, müssen die der adjungirten Gattung entnommenen Elemente so gewählt werden, dass sich alle aus dem Stammbereich hervorgehenden ganzen algebraischen Grössen des Gattungs-Bereichs als *ganze* Functionen derselben ausdrücken lassen; dies ist z. B. der Fall, wenn die sämmtlichen Elemente eines Fundamentalsystems der adjungirten Gattung unter die Elemente $\mathfrak{R}$ mit aufgenommen werden.

Jedes Fundamentalsystem kann auf seine nothwendigen Elemente beschränkt angenommen werden, d. h. auf diejenigen, von denen keines sich als homogene ganze lineare Function der übrigen so darstellen lässt, dass die Coefficienten ganze Functionen der Grössen $\mathfrak{R}$ werden. Die sämmtlichen Discriminanten von je n Elementen eines Fundamentalsystems bilden ein System von Discriminanten, welches — als Ganzes betrachtet — selbst, so zu sagen, fundamental ist. Auch gelangt man, wenn man das Quadrat der Determinante

$$|x_i^{(h)}| \qquad (h, i = 1, 2, \ldots n+m)$$

bildet, in welcher $x_1^{(h)}, x_2^{(h)}, \ldots x_n^{(h)}$ unter einander conjugirte algebraische Grössen und aber $x_{n+1}^{(h)}, x_{n+2}^{(h)}, \ldots x_{n+m}^{(h)}$ unbestimmte oder variable Grössen bedeuten, zu einer ganzen homogenen „Form" dieser $m(m+n)$ Variabeln, deren Coefficienten ein fundamentales System von Discriminanten bilden, und welche also dieses System vertritt. Ebenso wird dieses System von Discriminanten durch irgend eine lineare homogene Function derselben mit unbestimmten Coefficienten $u', u'', \ldots,$ d. h. also durch eine lineare homogene Form der Variabeln u repräsentirt, deren Coefficienten die verschiedenen Discriminanten eines Fundamentalsystems sind. Eine solche Linearform sowie überhaupt — wenn von jeder Darstellungsweise abstrahirt wird — *die Gesammtheit dessen, was den Discriminanten eines Fundamentalsystems und zugleich den als ganze homogene Functionen derselben* (mit ganzen rationalen dem Bereich $[\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots]$ angehörigen Coefficienten) *darstellbaren Grössen gemeinsam ist,* d. h. der Complex aller derjenigen Eigenschaften jener Discriminanten, welche für ganze homogene Verbindungen derselben erhalten bleiben, gehört offenbar *jeder* Discriminante von je n Functionen der Art, oder — wenn es die Haupt-Art ist — der Gattung an und bildet somit einen Complex von Eigenschaften, welche der Art oder der Gattung als solcher angehören, also einen Complex von „Invarianten" der Art oder Gattung im höheren Sinne des Wortes*).

Sind die Grössen $\mathfrak{R}$ die Elemente eines natürlichen Rationalitäts-Bereichs, d. h. also, kommen unter den Grössen $\mathfrak{R}$ keine algebraischen Grössen sondern nur unabhängige Variable vor, so giebt es stets eine ganze ganzzahlige Function derselben (für $\mathfrak{R} = 1$ eine ganze von *Eins* verschiedene

*) Vgl. § 25 und auch die Darlegung des allgemeineren Invarianten-Begriffs am Schlusse meines im Monatsbericht der Berliner Akademie vom April 1874 abgedruckten Aufsatzes.

Zahl), welche gemeinsamer Theiler aller Discriminanten des Fundamentalsystems und desshalb füglich (wie in meinem citirten Aufsatze vom April 1874) als „Discriminante der Art oder Gattung" bezeichnet werden kann. Dies findet nicht mehr immer statt, wenn eine Gattung algebraischer Grössen zum Rationalitäts-Bereich gehört, wenn dieser also ein Gattungs-Bereich ist. So haben, wie ich schon im Monatsberichte der Berliner Akademie vom Juni 1862 S. 368 erwähnt habe, die Gattungen singulärer Moduln der elliptischen Functionen die merkwürdige Eigenschaft, bei Adjunction von gewissen Quadratwurzeln, bei welcher die Gleichung der Moduln in Theilgleichungen zerfällt, keine „Discriminante der Gattung" mehr zu besitzen; so hat ferner die von mir im Monatsberichte der Berliner Akademie vom Juni 1861 S. 611 aufgestellte Gleichung

$$x^6 + 4ax^5 + 10bx^3 + 4cx - 4ac + 5b^2 = 0$$

die Eigenschaft, dass ihre Discriminante abgesehen vom Factor *Fünf* das Quadrat einer ganzen ganzzahligen Function der Grössen a, b, c ist, und dass bei Adjunction der Quadratwurzel aus dieser ganzen Function von a, b, c die durch eine Wurzel der Gleichung repräsentirte Gattung algebraischer Functionen der Grössen a, b, c keine Discriminante hat.

Giebt es Fundamentalsysteme von n Elementen, d. h. von genau so vielen als die Ordnung beträgt, so ist die Discriminante der Elemente des Fundamentalsystems selbst die Discriminante der Art oder Gattung, und diese allein repräsentirt dann die „Invariante". Ist die Anzahl der unabhängigen Variabeln $\mathfrak{R}$ gleich ν, so repräsentirt eine bestimmte Gattung algebraischer Functionen derselben eine ν-fache Mannigfaltigkeit, und die Discriminante der Gattung, gleich Null gesetzt, eine $(\nu-1)$-fache Mannigfaltigkeit. Aber nicht bloss diese $(\nu-1)$-fache Mannigfaltigkeit, sondern auch alle diejenigen weniger ausgedehnten Mannigfaltigkeiten, d. h. die $(\nu-2)$-fachen, $(\nu-3)$-fachen u. s. w., in welchen sämmtliche Discriminanten eines Fundamentalsystems von mehr als n Elementen zugleich Null werden, sind Invarianten der Gattung. Doch bleibt dahingestellt, ob solche Invarianten wirklich vorkommen.

Da jede einem Bereich $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$ entstammende algebraische Grösse sich als homogene lineare Function von n linear unabhängigen algebraischen Grössen der Gattung so ausdrücken lässt, dass die Coefficienten zum Rationalitäts-Bereich $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$ gehören, so stehen die Discriminanten von je n algebraischen Grössen der Gattung zu einander in

quadratischen Verhältnissen, d. h. in Verhältnissen von Quadraten rationaler Grössen des Bereichs. Was nach *Sylvester*scher Weise als Discriminante einer homogenen Form

$$c_n x^n + c_{n-1} x^{n-1} y + \cdots + c_1 x y^{n-1} + c_0 y^n$$

oder als Discriminante der Gleichung

$$c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0 = 0$$

bezeichnet wird, ist nach den obigen Definitionen die Discriminante der n algebraischen Grössen

$$c_n x^{n-1} + c_{n-1} x^{n-2} + \cdots + c_1, \quad c_n x^{n-2} + c_{n-1} x^{n-3} + \cdots + c_2, \quad \ldots, \quad c_n x + c_{n-1}, \quad 1,$$

welche sämmtlich *ganze* algebraische Functionen der $n+1$ Grössen c sind, wenn x eine Wurzel jener Gleichung n^{ten} Grades bedeutet. Die Discriminante aller derselben Gattung angehörigen Gleichungen*)

$$c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0 = 0,$$

in welchen die Coefficienten c offenbar als *ganze* rationale Grössen des Bereichs vorausgesetzt werden können, stehen also zu einander in quadratischen Verhältnissen und enthalten sämmtlich die Discriminante der Gattung als gemeinsamen Theiler. Dies ist freilich nicht immer der *grösste* gemeinsame Theiler; aber es lässt sich zeigen, dass nur ein Divisor einer gewissen *Potenz* der Discriminante der Gattung grösster gemeinsamer Theiler aller Gleichungs-Discriminanten sein kann. Der Nachweis dieser für die Theorie der algebraischen Gleichungen höchst wichtigen Eigenschaft der Discriminanten beruht auf folgendem elementaren Determinantensatze.

Wird das Product der $n(n-1)$ Differenzen von n homogenen linearen Functionen der Variabeln $u_1, u_2, \ldots u_n$

$$a_{11} u_1 + a_{12} u_2 + \cdots + a_{1n} u_n, \quad \ldots, \quad a_{n1} u_1 + a_{n2} u_2 + \cdots + a_{nn} u_n$$

nach den verschiedenen Producten von Potenzen der Grössen u entwickelt, so besteht für die dabei auftretenden Coefficienten $\Phi(a_{11}, \ldots a_{nn})$, welche ganze ganzzahlige Functionen der Coefficienten a_{ik} sind, eine Gleichung

$$\Sigma \Phi(a_{11}, \ldots a_{nn}) \Psi(a_{11}, \ldots a_{nn}) = |a_{ik}|^{n(n-1)} \qquad (i, k = 1, 2, \ldots n),$$

in welcher auch die Multiplicatoren Ψ ganze ganzzahlige Functionen der Coefficienten a_{ik} sind, und in welcher die Summation auf alle Coefficienten

*) Der Begriff der Gattung ist hier, wie im Monatsbericht der Berliner Akademie vom März 1879 S. 214, von den algebraischen Grössen auf die Gleichungen übertragen, durch welche sie definirt werden. — Die Discriminante der Gleichung, welcher eine ganze algebraische Grösse x genügt, habe ich früher kurz als Discriminante der Grösse x und den mit der Discriminante der Gattung identischen Theiler derselben als ihren „wesentlichen", den anderen als „ausserwesentlichen" Theiler bezeichnet.

Φ zu erstrecken ist. Dabei ist zu bemerken, dass die Functionen Φ und Ψ in Beziehung auf die verschiedenen Horizontalreihen der Coefficienten a_{ik} symmetrisch sind. Der Beweis dieses Satzes ergiebt sich unmittelbar, wenn

$$\sum_i a_{ik} u_i = |a_{ik}|\, v_k \qquad (i, k = 1, 2, \ldots n)$$

gesetzt wird, so dass, wenn die Grössen α_{ik} die Adjungirten der Grössen a_{ik} bedeuten, die Variabeln u sich durch die neuen Variabeln v mittels der Gleichungen

$$\sum_i \alpha_{ik} v_i = u_k \qquad (i, k = 1, 2, \ldots n)$$

bestimmen. Dann ist nämlich

$$|a_{ik}|^{n(n-1)}\, \Pi(v_g - v_h) = \Sigma \Phi_{r_1, r_2, \ldots r_n} u_1^{r_1} u_2^{r_2} \ldots u_n^{r_n} \qquad (i, k = 1, 2, \ldots n),$$

wo sich das Productzeichen links auf alle unter einander verschiedenen Werthe $g, h = 1, 2, \ldots n$ und das Summationszeichen rechts auf alle Exponenten-Systeme $r_1, r_2, \ldots r_n$ bezieht, und diese Gleichung wird eine Identität, wenn man die Grössen u auf der rechten Seite durch die linearen Functionen $\Sigma \alpha_{1i} v_i$, $\Sigma \alpha_{2i} v_i$, $\ldots$ ersetzt. Werden alsdann auf beiden Seiten die Coefficienten des Gliedes $v_1^{n-1} . v_2^{n-2} \ldots v_{n-1}$ mit einander verglichen, so resultirt jene Gleichung

$$|a_{ik}|^{n(n-1)} = \Sigma \Phi(\alpha_{11}, \ldots \alpha_{nn})\, \Psi(a_{11}, \ldots a_{nn}),$$

da auf der rechten Seite jeder der Coefficienten $\Phi_{r_1, r_2, \ldots r_n}$ mit einer ganzen ganzzahligen Function der Adjungirten von $a_{11}, \ldots a_{nn}$, also in der That mit einer ganzen ganzzahligen Function dieser Grössen selbst multiplicirt erscheint.

Nimmt man nunmehr an Stelle der n^2 Grössen a_{ik} die ganzen algebraischen Grössen $x_i^{(k)}$, d. h. n conjugirte Reihen von je n Elementen, so bilden die mit Φ bezeichneten Ausdrücke die Coefficienten der Entwickelung der Discriminante von

$$u_1 x' + u_2 x'' + \cdots + u_n x^{(n)}$$

nach Producten der Potenzen von $u_1, u_2, \ldots u_n$. Die Grössen Φ sind demnach *ganze* rationale Grössen des Bereichs, und deren grösster gemeinsamer Theiler muss nach obigem Satze ein Theiler der $\frac{1}{2}n(n-1)^{\text{ten}}$ Potenz der Discriminante der n Elemente

$$x', \quad x'', \quad \ldots \quad x^{(n)}$$

sein. Bilden ferner, wie oben, die $n+m$ ganzen algebraischen Grössen

$$x', \quad x'', \quad \ldots \quad x^{(n+m)}$$

ein Fundamentalsystem, so repräsentirt der lineare Ausdruck mit unbestimmten Coefficienten

$$u_1 x' + u_2 x'' + \cdots + u_{n+m} x^{(n+m)}$$

die allgemeinste ganze algebraische Grösse der Gattung, und die Discriminante der Gleichung, der dieser Ausdruck genügt, kann keinen von den Grössen u unabhängigen Theiler haben, der nicht ein Divisor der $\frac{1}{2}n(n-1)^{\text{ten}}$ Potenzen aller Discriminanten von je n Elementen x, d. h. also ein Divisor der $\frac{1}{2}n(n-1)^{\text{ten}}$ Potenz der Discriminante der Gattung wäre. Dies ist der eigentliche Zielpunkt der vorstehenden Entwickelung. Es folgt daraus, dass alle Discriminanten der verschiedenen Gleichungen der Gattung, d. h. alle die Discriminanten, welche man erhält, wenn man den Grössen u alle möglichen Werthe beilegt, keinen Divisor gemein haben können, der nicht zugleich Divisor der $\frac{1}{2}n(n-1)^{\text{ten}}$ Potenz der Discriminante der Gattung wäre, sofern nämlich eine ganze Function der unbestimmten Grössen u, welche keinen von denselben unabhängigen Theiler enthält, durch geeignete Bestimmung von $u_1, u_2, \ldots u_{n+m}$ so eingerichtet werden kann, dass sie mit einer gegebenen ganzen rationalen Function von $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots$ keinerlei gemeinsamen Theiler hat. Dies ist stets möglich, wenn wenigstens eine Variable unter den Grössen $\mathfrak{R}$ vorkommt, während allerdings für $\mathfrak{R} = 1$ z. B. der Ausdruck $u^p - u$, obgleich ohne einen von u unabhängigen Factor, doch falls p Primzahl ist, für jeden ganzzahligen Werth von u durch p theilbar wird (vgl. § 25).

Im Vorhergehenden ist vielfach von Theilern und namentlich von „grössten gemeinschaftlichen Theilern" ganzer rationaler Functionen von $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots$ die Rede gewesen. Für natürliche Rationalitäts-Bereiche ist dies durch die in § 4 nachgewiesene Möglichkeit der Zerlegung ganzer ganzzahliger Functionen von Variabeln in irreductible Factoren völlig gerechtfertigt; für die Gattungs-Bereiche aber bedarf es des Hinweises auf die erst im zweiten Theile folgende Begründung.

§ 9.

Die Beziehungen zwischen Discriminanten verschiedener Gattungen, von denen die eine unter der anderen enthalten ist.

Repräsentirt die ganze algebraische Grösse x eine Gattung n^{ter} Ordnung und die ganze algebraische Grösse y eine Gattung mn^{ter} Ordnung, unter welcher die erstere enthalten ist, so theilen sich die mn conjugirten

Grössen y in n Gruppen von je m Grössen. Jede von diesen n Gruppen besteht aus denjenigen m Grössen y, welche bei Adjunction einer bestimmten der n conjugirten Grössen x mit einander conjugirt bleiben. Die Gleichung mn^{ten} Grades, welcher y genügt, zerfällt nämlich in n Gleichungen m^{ten} Grades, welche gewissermassen mit einander conjugirt sind; denn es ist, wenn die zu x_k gehörige Gruppe von Grössen y mit $y_{1k}, y_{2k}, \dots y_{mk}$ bezeichnet wird,

$$(y-y_{1k})(y-y_{2k})\dots(y-y_{mk}) = G(y, x_k),$$

wo $G(y, x)$ eine ganze Function von y und x bedeutet, deren Coefficienten dem Rationalitäts-Bereich $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \dots)$ angehören, und die Gleichung

$$\prod_k G(y, x_k) = 0 \qquad (k=1,2,\dots n)$$

ist also diejenige Gleichung mn^{ten} Grades, durch welche die algebraische Grösse y definirt wird. Bildet man nun für irgend eine Reihe ganzer algebraischer Grössen $y', y'', y''', \dots y^{(r)}$ der durch y bezeichneten Gattung die mn Reihen conjugirter Grössen

$$y'_{ik}, \quad y''_{ik}, \quad y'''_{ik}, \quad \dots \quad y^{(r)}_{ik} \qquad (i=1,2,\dots m;\ k=1,2,\dots n)$$

und ersetzt alsdann in diesem Grössensystem jede der n Reihen

$$y'_{1k}, \quad y''_{1k}, \quad y'''_{1k}, \quad \dots \quad y^{(r)}_{1k} \qquad (k=1,2,\dots n)$$

durch die Reihe von Summen

$$\sum_{i=1}^{i=m} y'_{ik}, \quad \sum_{i=1}^{i=m} y''_{ik}, \quad \sum_{i=1}^{i=m} y'''_{ik}, \quad \dots \quad \sum_{i=1}^{i=m} y^{(r)}_{ik} \qquad (k=1,2,\dots n),$$

welche sämmtlich Grössen der Gattung x_k sind, so entsteht ein System von mn Reihen von je r Elementen, unter denen n Reihen beziehungsweise den n conjugirten Gattungen $x_1, x_2, \dots x_n$ angehören. Hieraus geht hervor, dass die Discriminante von je mn ganzen algebraischen Grössen der Gattung y sich als lineare homogene Function von Discriminanten der Gattung x so darstellen lässt, dass die Coefficienten ganze algebraische Grössen sind. Jede der „Invarianten" der Gattung x ist also gewissermassen in den „Invarianten" der Gattung y enthalten, und namentlich ist *die Discriminante der Gattung x ein Theiler der Discriminante der Gattung y, unter welcher jene enthalten ist.* Da ferner jede Discriminante von je n Grössen der Gattung y durch die Discriminante der Gattung theilbar ist, so folgt, *dass die Discriminante einer Gattung algebraischer Grössen x Divisor der Discri-*

minante einer jeden (auch reductibeln) Gleichung ist, welche die Eigenschaft hat, dass sich durch eine ihrer Wurzeln die Grössen jener Gattung x rational ausdrücken lassen.

§ 10.

Die Systeme von Gleichungen; ihre Discriminanten und ihre verschiedenen Resolventen.

Der oben entwickelte Begriff der Discriminante der Gattung findet vielfache Anwendung in der Theorie der Elimination, und eine der wichtigsten dieser Anwendungen soll hier kurz erwähnt werden. — Bedeuten F_1, $F_2, \ldots F_n$ ganze homogene Functionen der $n+1$ Variabeln $x^0, x', x'', \ldots x^{(n)}$, welche vollständige Ausdrücke der Dimensionen $r_1, r_2, \ldots r_n$ sind, so werden durch das Gleichungssystem

$$F_1 = 0, \quad F_2 = 0, \quad \ldots \quad F_n = 0$$

die Verhältnisse der $n+1$ Grössen x als algebraische Functionen der Coefficienten von $F_1, F_2, \ldots F_n$ definirt. Alle diese algebraischen Functionen gehören einer bestimmten Gattung an, und die Discriminante dieser Gattung ist eine ganze ganzzahlige Function jener Coefficienten, welche auch in folgender Weise, unabhängig von den obigen allgemeinen Entwickelungen, erklärt werden kann. Bedeutet F_0 eine ganz beliebige (z. B. eine lineare) homogene Function der $n+1$ Grössen x mit unbestimmten Coefficienten, so hat die Eliminations-Resultante der $n+1$ homogenen Gleichungen

$$F_1 = 0, \quad F_2 = 0, \quad \ldots \quad F_n = 0, \quad |F_{gh}| = 0 \qquad (g, h = 0, 1, \ldots n)$$

einen von den Coefficienten der Function F_0 unabhängigen Factor, welcher füglich als die Discriminante des Functionen-Systems $(F_1, F_2, \ldots F_n)$ oder des Gleichungssystems

$$F_1 = 0, \quad F_2 = 0, \quad \ldots \quad F_n = 0$$

zu bezeichnen ist und mit jener Discriminante der Gattung genau übereinstimmt. Nur für das Vorzeichen derselben bedürfte es noch einer besonderen Bestimmung.

Die Discriminante des Functionen-Systems $(F_1, F_2, \ldots F_n)$ ist irreductibel, wie ich in einer anderen Abhandlung beweisen werde. Das Verschwinden derselben enthält die nothwendige und hinreichende Bedingung dafür, dass zwei den Gleichungen $F=0$ genügende Werthsysteme mit einander identisch werden.

Die Behandlung ganz allgemeiner Gleichungssysteme, welche hier einen zu grossen Raum einnehmen würde, behalte ich einem besonderen

Aufsatze vor; doch muss hier eine Andeutung der Methode und eine Angabe der Hauptresultate ihren Platz finden, weil ich mich in den folgenden Paragraphen darauf zu beziehen haben werde. Ein System von beliebig vielen algebraischen Gleichungen für $z^0, z', z'', \ldots z^{(n-1)}$, in welchen die Coefficienten dem Rationalitäts-Bereich $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$ angehören, definirt algebraische Beziehungen zwischen den Grössen z und $\mathfrak{R}$, deren Erkenntniss und Darlegung den Zielpunkt der Theorie der Elimination bildet. Die m Functionen $G_1, G_2, \ldots G_m$, welche, gleich Null gesetzt, die Gleichungen bilden, sind als ganze rationale Functionen der n Grössen z vorauszusetzen, deren Coefficienten aber nur als rationale (ganze oder gebrochene) Functionen der Grössen $\mathfrak{R}$ mit ganzzahligen Coefficienten. Für die Anzahl der Functionen, welche mit m bezeichnet ist, soll keinerlei Beschränkung angenommen werden; sie kann, wie im obigen speciellen — dem sogenannten allgemeinen — Falle, gleich n, d. h. gleich der Anzahl der zu bestimmenden Grössen z, aber auch grösser oder kleiner als diese Zahl n sein. Werden die Grössen z als unbeschränkt veränderlich aufgefasst, so constituiren die Gleichungen $G = 0$ eine gewisse Beschränkung dieser Variabilität, deren nähere Charakterisirung als die Aufgabe der Elimination bezeichnet werden kann. Dabei ist aber die Unbestimmtheit der etwaigen unbestimmten Grössen $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots$ oder, falls diese als Variable aufgefasst werden, die uneingeschränkte Variabilität derselben festzuhalten, d. h. es ist nur diejenige Beschränkung der Variabilität der Grössen z zu charakterisiren, welche keinerlei Beschränkung der Variabilität der Grössen $\mathfrak{R}$ erfordert. Die hier präcisirte Unterscheidung zwischen den Variabeln z und denen, die unter den Grössen $\mathfrak{R}$ vorkommen, ist von der grössten Wichtigkeit; sie involvirt keinerlei Beschränkung der Allgemeinheit, sondern sie scheidet nur die verschiedenen Aufgaben, welche bei der Elimination gestellt werden können, nach ihrem begrifflichen Inhalt. (Vgl. die Unterscheidung zwischen den Unbestimmten u und den Variabeln $\mathfrak{R}$ in den Conclusionen des § 22.)

Um die Functionen G von Zufälligkeiten zu befreien, ist auf die Grössen z eine allgemeine lineare Transformation anzuwenden, deren Specialisation vorbehalten bleibt. Werden die n transformirten Variabeln mit $x', x'', \ldots x^{(n)}$ bezeichnet, so ist nunmehr an Stelle von $x^{(n)}$ eine lineare Function

$$u_1 x' + u_2 x'' + \cdots + u_n x^{(n)}$$

mit unbestimmten Coefficienten u einzuführen, die mit x bezeichnet werden

möge. Hiernach treten an Stelle der m Gleichungen $G=0$ ebensoviel Gleichungen

$$H_1=0,\quad H_2=0,\quad \ldots\quad H_m=0,$$

in welchen $H_1, H_2, \ldots H_m$ ganze Functionen von $x, x', x'', \ldots x^{(n-1)}$ und deren Coefficienten rationale Functionen der Grössen u und $\mathfrak{R}$ sind. Diese können überdies als *ganz* in Beziehung auf $u_1, \ldots u_n$ vorausgesetzt werden, da, um diese Voraussetzung zu erfüllen, nur mit einer Potenz von u_n multiplicirt zu werden braucht. Jede der Functionen H kann ferner von etwaigen gleichen Factoren befreit gedacht werden. Endlich kann der grösste gemeinsame Theiler aller Functionen H herausgehoben werden. Dieser sei

$$F_1(x, x', x'', \ldots x^{(n-1)}),$$

und der Quotient der Division von H_α durch F_1 sei K_α; alsdann ist das System der Gleichungen $H=0$, abgesehen von dem Inhalte der Gleichung $F_1=0$, äquivalent dem Systeme der Gleichungen $K=0$. Bildet man nun zwei lineare Verbindungen der letzteren m Gleichungen

$$U_1K_1+U_2K_2+\cdots+U_mK_m=0,\quad V_1K_1+V_2K_2+\cdots+V_mK_m=0,$$

entwickelt die aus der Elimination von $x^{(n-1)}$ hervorgehende Resultante nach Producten von Potenzen der unbestimmten Grössen U, V, und setzt alle einzelnen Coefficienten gleich Null, so gelangt man zu einem Gleichungssystem für die $n-1$ Grössen $x, x', x'', \ldots x^{(n-2)}$, welches zum neuen Ausgangspunkt genommen werden kann. Es wird demgemäss der grösste gemeinsame Theiler aller jener Coefficienten der Resultante, nachdem derselbe von etwaigen gleichen Factoren befreit ist, mit $F_2(x, x', x'', \ldots x^{(n-2)})$ zu bezeichnen sein, und allmählich bei wiederholter Anwendung des angegebenen Verfahrens eine Reihe von Functionen

$$F_1(x, x', x'', \ldots x^{(n-1)}),\quad F_2(x, x', x'', \ldots x^{(n-2)}),\quad \ldots\quad F_n(x)$$

sich ergeben, welche, gleich Null gesetzt, ein dem ursprünglichen System $G=0$ äquivalentes Gleichungssystem bilden. Die Productgleichung

$$F_1.F_2.\ldots.F_n = 0$$

ist die Gesammtresolvente des Gleichungssystems $G=0$; jede Theilresolvente $F_k=0$ repräsentirt eine durch die Gleichungen $G=0$ aus der gesammten n-fachen Mannigfaltigkeit $(\mathfrak{z})$ ausgeschiedene $(n-k)$-fache Mannigfaltigkeit, also ein $(n-k)$-fach ausgedehntes Gebilde, und es kann daher im Allgemeinen durch irgend ein Gleichungssystem $G=0$ eine Anzahl von Gebilden jeglicher Ausdehnung, Punkten, Linien u. s. w., d. h. eine Anzahl nullfacher, einfacher, zweifacher, ... $(n-1)$-facher Mannigfaltigkeiten $(\mathfrak{z})$ *simultan* definirt werden.

Die Functionen F_k sind sämmtlich, als Functionen von $u_1, u_2, \dots u_n$, in lineare Factoren zerlegbar. Jeder Linearfactor von F_k ergiebt, gleich Null gesetzt, die letzten k Grössen x, nämlich $x^{(n-k+1)}, x^{(n-k+2)}, \dots x^{(n)}$ als algebraische Functionen der ersten $n-k$ Grössen $x', x'', \dots x^{(n-k)}$; denn ein solcher Linearfactor hat die Form

$$x - u_1\varphi' - u_2\varphi'' - \dots - u_n\varphi^{(n)},$$

wo $\varphi', \varphi'', \dots \varphi^{(n)}$ algebraische Functionen von $x', x'', \dots x^{(n-k)}$ bedeuten, und es sind dabei die ersten $n-k$ Grössen φ beziehungsweise mit den ersten $n-k$ Grössen x selbst identisch, so dass bei Einsetzung des Werthes von x nur ein Aggregat

$$u_{n-k+1}(x^{(n-k+1)} - \varphi^{(n-k+1)}) + \dots + u_n(x^{(n)} - \varphi^{(n)})$$

verbleibt, welches, gleich Null gesetzt, wegen der Unbestimmtheit der Grössen u den Complex der k Gleichungen

$$x^{(n-k+1)} = \varphi^{(n-k+1)}, \quad \dots \quad x^{(n)} = \varphi^{(n)}$$

und also eine $(n-k)$-fache Mannigfaltigkeit darstellt. Weil hiernach die Theilresolvente $F_k = 0$ ein System von k Gleichungen vertritt, soll die Function F_k so wie die Gleichung $F_k = 0$ als eine von „*k^{ter} Stufe*" bezeichnet werden.

Die einzelnen Functionen F_k können, als Functionen von $x, x', \dots x^{(n-k)}$ betrachtet, mit Berücksichtigung des Rationalitäts-Bereichs $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \dots)$ in irreductible Factoren zerlegt gedacht werden. Jeder dieser irreductibeln Factoren, sowie überhaupt jeder Theiler Φ des Products $F_1F_2\dots F_n$ stellt, gleich Null gesetzt, die Gesammtresolvente eines gewissen Gleichungssystems dar. Man erhält dasselbe, indem man in dem herausgehobenen Theiler jenes Products Φ die Grösse x wieder durch ihren Werth

$$u_0x^0 + u_1x' + \dots + u_{n-1}x^{(n-1)}$$

ersetzt und alsdann den Grössen u eine Anzahl bestimmter Werthsysteme beilegt. Man sieht dabei leicht, dass stets $n+1$ solcher Werthsysteme ausreichen, damit die hieraus entstehenden Gleichungen

$$\Phi_1 = 0, \quad \Phi_2 = 0, \quad \dots \quad \Phi_{n+1} = 0$$

die Gesammtresolvente $\Phi = 0$ haben, und es ergiebt sich daher das Resultat,

> dass der gesammte Inhalt jedes Theilers der Resolvente eines Gleichungssystems für n Grössen x durch ein System von nur $n+1$ Gleichungen dargestellt, also auch jedes System von beliebig vielen Gleichungen durch ein solches von nur $n+1$ Gleichungen ersetzt werden kann.

Die „Ordnung“ eines Gleichungssystems wird durch den Grad seiner Resolvente bezeichnet. Das Gleichungssystem heisst irreductibel, wenn die Resolvente irreductibel ist. Stellt das irreductible Gleichungssystem ein $(n-k)$-fach ausgedehntes Gebilde dar, so ist es unmöglich, nur einen ebenfalls $(n-k)$-fach ausgedehnten *Theil* desselben durch ein algebraisches Gleichungssystem auszudrücken. Auch für eine Resolvente $F_n = 0$, welche nur einzelne Punkte der n-fachen Mannigfaltigkeit (z) darstellt, behält der Begriff der Irreductibilität mit Rücksicht auf den angenommenen Rationalitäts-Bereich seine Bedeutung. Nur von den Potenzen irreductibler Resolventen ist bei der vorstehenden Betrachtung gänzlich abgesehen, da ja schon bei der Methode der Bildung die Befreiung von gleichen Factoren Bedingung war.

Derjenige Theil der Resolvente eines beliebigen Gleichungssystems, welcher eine $(n-k)$-fache Mannigfaltigkeit (z) repräsentirt, drückt eine zwischen $n-k+1$ Grössen x bestehende Beziehung

$$F_k(x, x', x'', \dots x^{(n-k)}) = 0$$

aus, während die n Variabeln z durch diese $n-k+1$ Grössen x und durch die Grössen u und $\mathfrak{R}$ rational darstellbar sind. Auch können den unbestimmten Grössen u solche *speciellen* Werthe beigelegt werden, dass diese Art der Darstellbarkeit erhalten bleibt. Bezeichnet man die Function F_k für derartige specielle Werthe der Grössen u mit Φ, so repräsentirt die Gleichung $\Phi = 0$ eine aus der $(n-k+1)$-fachen Mannigfaltigkeit $x, x', x'', \dots x^{(n-k)}$ ausgesonderte $(n-k)$-fache Mannigfaltigkeit, auf welche jene aus der n-fachen Mannigfaltigkeit (z) ausgesonderte $(n-k)$-fache Mannigfaltigkeit eindeutig bezogen ist. Es lässt sich daher jedes m-fach ausgedehnte Gebilde einer beliebig grossen Mannigfaltigkeit auf ein solches eindeutig beziehen, das aus einer nur $(m+1)$-fachen Mannigfaltigkeit entnommen ist.

Es ist schliesslich als ein Hauptresultat der allgemeinen Eliminationstheorie hervorzuheben, dass der in § 2 an die Betrachtung einer einzigen Gleichung geknüpfte Begriff der algebraischen Grösse keinerlei Erweiterung bedarf, wenn Systeme von Gleichungen mit in den Kreis der Betrachtung gezogen werden. Sind nämlich eine Anzahl Grössen zusammen durch eine beliebige Anzahl von algebraischen Gleichungen definirt, deren Coefficienten dem Rationalitäts-Bereich $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \dots)$ angehören, so ist, wie aus der Theorie der Elimination hervorgeht, jede einzelne der so definirten Grössen eine algebraische Function von $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \dots$ auch in dem *engeren* in § 2 angegebenen Sinne des Wortes.

§ 11.

Die besonderen Gleichungssysteme, durch welche conjugirte algebraische Grössen definirt werden. Das *Galois*sche algebraische Princip.

Die allgemeine Theorie der Elimination, wie sie im vorhergehenden Paragraphen skizzirt worden ist, zeigt die eigentliche Quelle des neuen Lichts, welches gerade vor einem halben Jahrhundert durch *Galois* in die Theorie der algebraischen Gleichungen gebracht worden ist.

Es seien $c_1, c_2, \ldots c_n$ Grössen des Rationalitäts-Bereichs $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$ und

$$(A) \qquad x^n - c_1 x^{n-1} + c_2 x^{n-2} - \cdots \pm c_n = 0$$

eine irreductible Gleichung mit den Wurzeln $\xi_1, \xi_2, \ldots \xi_n$, welche also conjugirte algebraische Functionen der Grössen $\mathfrak{R}$ sind. Es seien ferner

$$\mathfrak{f}_1(x_1, x_2, \ldots x_n), \quad \mathfrak{f}_2(x_1, x_2, \ldots x_n), \quad \ldots \quad \mathfrak{f}_n(x_1, x_2, \ldots x_n)$$

die n durch die identische Gleichung

$$(x-x_1)(x-x_2)\ldots(x-x_n) = x^n - \mathfrak{f}_1 x^{n-1} + \mathfrak{f}_2 x^{n-2} - \cdots \pm \mathfrak{f}_n$$

definirten „elementaren symmetrischen“ Functionen von $x_1, x_2, \ldots x_n$. Alsdann kann man die n Grössen ξ, ebenso wie durch die *eine* Gleichung (A), auch durch das System von n Gleichungen

$$(B) \qquad \mathfrak{f}_k(\xi_1, \xi_2, \ldots \xi_n) = c_k \qquad (k=1,2,\ldots n)$$

bestimmt ansehen, und es ist diese höhere Auffassung der in einer algebraischen Gleichung enthaltenen Bestimmungen, welche — wenn auch nicht geradezu ausgesprochen — der *Galois*schen Behandlung der algebraischen Gleichungen zu Grunde liegt. Um dies zu erkennen, braucht man nur das besondere, n *conjugirte* algebraische Grössen definirende Gleichungssystem

$$(C) \qquad \mathfrak{f}_k(x_1, x_2, \ldots x_n) = c_k \qquad (k=1,2,\ldots n)$$

nach der allgemeinen im vorhergehenden Paragraphen entwickelten Methode zu behandeln.

Das Gleichungssystem

$$(C) \qquad \mathfrak{f}_k(x_1, x_2, \ldots x_n) = c_k \qquad (k=1,2,\ldots n)$$

kann nur eine Resolvente n^{ter} Stufe haben, da ja aus diesem Gleichungssystem auch das folgende hervorgeht

$$(\bar{A}) \qquad x_k^n - c_1 x_k^{n-1} + c_2 x_k^{n-2} - \cdots \pm c_n = 0 \qquad (k=1,2,\ldots n).$$

Hierbei ist jedoch hervorzuheben, dass die beiden Gleichungssysteme (C) und $(\bar{A})$

keineswegs äquivalent sind; sondern das letztere, welches von der Ordnung n^n ist, enthält das erstere, welches nur von der Ordnung $n!$ ist.

Bedeutet nun $F(x)=0$ die Resolvente des Gleichungssystems (C) und ist

$$x = u_1 x_1 + u_2 x_2 + \cdots + u_n x_n,$$

so sind die Coefficienten von $F(x)$ ganze Functionen der Unbestimmten $u_1, u_2, \ldots u_n$ und rationale Functionen der Grössen $\mathfrak{R}$. Da die Gleichungen (C) nur durch Werthsysteme

$$x_1 = \xi_{r_1}, \quad x_2 = \xi_{r_2}, \quad \ldots \quad x_n = \xi_{r_n}$$

erfüllt werden können, wo $r_1, r_2, \ldots r_n$ gewisse Permutationen der Zahlen $1, 2, \ldots n$ bedeuten, so muss $F(x)$ gleich dem über alle diese Permutationen erstreckten Producte

$$\Pi(x - u_1\xi_{r_1} - u_2\xi_{r_2} - \cdots - u_n\xi_{r_n})$$

sein. Aber nicht bloss das Gleichungssystem (C) selbst, sondern auch jedes andere, welches durch Hinzufügung irgend welcher Gleichungen entsteht und mit $(\bar{C})$ bezeichnet werden möge, kann nur eine eben solche Resolvente

$$\Pi(x - u_1\xi_{r_1} - u_2\xi_{r_2} - \cdots - u_n\xi_{r_n}) = 0$$

haben. Also, welche Gleichungen auch für $x_1, x_2, \ldots x_n$ bestehen mögen, stets muss, sobald nur n Gleichungen (C) daraus abzuleiten sind, die Resolvente von der angegebenen Art sein. Bezeichnet man nunmehr mit

$$G(x, \mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n) = 0$$

die *Galois*sche Gleichung, deren $n!$ Wurzeln durch

$$x = u_1 x_{i_1} + u_2 x_{i_2} + \cdots + u_n x_{i_n}$$

für sämmtliche $n!$ Permutationen $i_1, i_2, \ldots i_n$ repräsentirt werden, so sind die Coefficienten der mit G bezeichneten Function von $x, \mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n$ ganze ganzzahlige Functionen von $u_1, u_2, \ldots u_n$. Irgend einer der irreductibeln Factoren von $G(x, c_1, c_2, \ldots c_n)$ muss daher, gleich Null gesetzt, die Resolvente des Gleichungssystems (C) repräsentiren. Ein solcher Factor ist also eine ganze Function von x und den Unbestimmten $u_1, u_2, \ldots u_n$ mit Coefficienten des Rationalitäts-Bereichs $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$ und möge mit

$$g(x, u_1, u_2, \ldots u_n)$$

bezeichnet werden. Dann ist gemäss den oben eingeführten Bezeichnungen

$$g(x, u_1, u_2, \ldots u_n) = \Pi(x - u_1\xi_{r_1} - u_2\xi_{r_2} - \cdots - u_n\xi_{r_n}),$$

oder wenn die Linearfactoren des Products — statt nach $u_1, u_2, \ldots u_n$ —

nach $\xi_1, \xi_2, \ldots \xi_n$ geordnet werden,

$$g(x, u_1, u_2, \ldots u_n) = \Pi(x - u_{r_1}\xi_1 - u_{r_2}\xi_2 - \cdots - u_{r_n}\xi_n).$$

Es ist daher

> $g(x, u_1, u_2, \ldots u_n)$, als Function der Unbestimmten $u_1, u_2, \ldots u_n$ betrachtet, eine solche, die bei gewissen durch $r_1, r_2, \ldots r_n$ bezeichneten Permutationen ungeändert bleibt,

und man gelangt somit, von irgend einer *speciellen* Gleichung (A) ausgehend, zu allgemeinen Functionen von n unbestimmten Grössen, welche die Eigenschaft haben, bei gewissen Permutationen derselben ihren Werth unverändert beizubehalten. Hierin liegt die grosse Bedeutung des *Galois*schen algebraischen Princips, anstatt einer einzigen Gleichung das die conjugirten Wurzeln gleichzeitig definirende *Gleichungssystem* der Untersuchung zu Grunde zu legen. *Galois* selbst hat es klar erkannt, dass seine neue Auffassung der algebraischen Gleichungen es möglich macht, von jeder einzelnen Gleichung mit ganz speciellen Coefficienten, z. B. von jeder Zahlengleichung, die für die algebraische Theorie einzig wesentlichen Eigenschaften *) zu abstrahiren, und er hat diese zur wahren Erkenntniss führende Methode dadurch vollständig dargelegt, dass er gezeigt hat, wie jeder speciellen Gleichung eine von der Werth-Bedeutung der Coefficienten oder Wurzeln unabhängige Eigenschaft in der von ihm so genannten „Gruppe der Substitutionen" zukommt. Nur scheint mir, dass der *Galois*schen Theorie noch eine weitere *formale* Ausbildung durch die leichte hier eingeführte Modification zu geben ist, bei welcher an Stelle der abstracten Substitutionen und deren Gruppen die concreten bei einer Gruppe von Permutationen unveränderlichen Functionen behandelt werden.

§ 12.

Die Gattungen rationaler Functionen mehrerer unbestimmten Grössen.

Nachdem gezeigt worden ist, wie das *Galois*sche Princip für jede specielle algebraische Gleichung eine für dieselbe charakteristische ganze Function von n Unbestimmten u ergiebt, können diese Functionen selbst

*) Die Bedingungen, unter denen die nach dem *Galois*schen Princip sich ergebenden Eigenschaften der algebraischen Gleichungen, welche ich als „Affecte" bezeichne, in der That die einzigen sind, werde ich in einem folgenden Aufsatze vollständig entwickeln.

zum Ausgangspunkt der Entwickelung genommen werden. Setzt man x_1, $x_2, \dots x_n$ an Stelle der Unbestimmten $u_1, u_2, \dots u_n$, so sind also ganze Functionen der n unbestimmten Grössen x in Beziehung auf die Veränderungen zu untersuchen, welche sie erfahren, wenn die Grössen x darin auf alle möglichen Weisen permutirt werden. Diese Untersuchung ordnet sich aber naturgemäss in die arithmetische Theorie der algebraischen Grössen ein, sobald man die ganzen Functionen von $x_1, x_2, \dots x_n$ als algebraische Functionen der n elementaren symmetrischen Functionen $\mathfrak{f}_1, \mathfrak{f}_2, \dots \mathfrak{f}_n$ auffasst, und hiermit wird also die Stelle bezeichnet, an welcher die *Galois*schen Resultate sich in die allgemeine Theorie einfügen.

Werden die n Functionen $\mathfrak{f}_1, \mathfrak{f}_2, \dots \mathfrak{f}_n$ an Stelle von $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \dots$ genommen, so dass $(\mathfrak{f}_1, \mathfrak{f}_2, \dots \mathfrak{f}_n)$ den Rationalitäts-Bereich bezeichnet, so ist jede rationale Function von $x_1, x_2, \dots x_n$ eine aus dem Bereich hervorgehende algebraische Function und gehört als solche einer bestimmten Gattung an, welche nun einfach als *„Gattung von Functionen von* $x_1, x_2, \dots x_n$" bezeichnet werden soll *). Der Begriff „conjugirt", sowie der Begriff der Ordnung soll auf diese Gattungen von Functionen übertragen werden, und auch der Begriff der „Art" kann bei den *ganzen* Functionen von $x_1, x_2, \dots x_n$ Anwendung finden.

Jede der einzelnen Grössen x repräsentirt eine Gattung n^{ter} Ordnung; durch eine lineare Function

$$u_1 x_1 + u_2 x_2 + \cdots + u_n x_n$$

mit unbestimmten Coefficienten u wird die „*Galois*sche Gattung" repräsentirt, welche von der Ordnung $n!$ ist und alle andern Gattungen unter sich enthält. Die Ordnungen der einzelnen Gattungen sind hiernach Theiler von $n!$, und wenn eine Gattung mit $\mathfrak{g}$, deren Ordnung mit ϱ und der Quotient $\frac{n!}{\varrho}$ mit r bezeichnet wird, so ist r die Anzahl der *„Permutationen der Gattung* $\mathfrak{g}$", d. h. die Anzahl *derjenigen Permutationen von* $x_1, x_2, \dots x_n$, bei denen eine Function der Gattung $\mathfrak{g}$ ungeändert bleibt. Ist die Gattung $\mathfrak{g}$ unter der Gattung $\mathfrak{g}'$ enthalten, so ist ϱ ein Theiler von ϱ' und also r', d. h. die Anzahl der Permutationen von $\mathfrak{g}'$, ein Theiler der mit r bezeichneten Anzahl der Permutationen von $\mathfrak{g}$, und es sind offenbar die ersteren Permutationen selbst unter den letzteren enthalten.

*) Vgl. meinen mehrerwähnten Aufsatz im Monatsbericht vom März 1879, aus welchem hier auch einige Stellen wörtlich aufgenommen sind.

Die Gattungen scheiden sich in *„eigentliche“* Gattungen von Functionen von n Grössen und in *„uneigentliche“*, je nachdem unter deren Adjunction die Gleichung $x^n - \mathfrak{f}_1 x^{n-1} + \mathfrak{f}_2 x^{n-2} - \cdots \pm \mathfrak{f}_n = 0$ irreductibel bleibt oder reductibel wird. Die uneigentlichen Gattungen lassen sich also auf Gattungen von Functionen von weniger als n Grössen zurückführen.

Werden die einer *eigentlichen* Gattung $\mathfrak{g}$ angehörigen Functionen den symmetrischen adjungirt, und wird demgemäss an Stelle des Rationalitäts-Bereichs $(\mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n)$ der erweiterte Bereich $(\mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n, \mathfrak{g})$ festgesetzt, so ändert sich damit der algebraische Charakter der durch die Gleichung

$$x^n - \mathfrak{f}_1 x^{n-1} + \mathfrak{f}_2 x^{n-2} - \cdots \pm \mathfrak{f}_n = 0$$

definirten algebraischen Function, und sie tritt damit in eine besondere „Classe“ von algebraischen Grössen ein. Die auf diese Weise definirten Classen algebraischer Functionen umfassen die einzelnen Gattungen. Ueberträgt man die Begriffe der Gattung und Classe von den algebraischen Functionen auf die Gleichungen, denen sie genügen, so gehören bei Festsetzung eines bestimmten Rationalitäts-Bereichs $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$ alle diejenigen irreductibeln Gleichungen $\Phi(x) = 0$ in eine und dieselbe Gattung, welche durch rationale Substitution von x aus einander entstehen, und alle diejenigen in dieselbe Classe, bei welchen die einer bestimmten Gattung $\mathfrak{g}$ angehörigen Functionen der Wurzeln zugleich dem festgesetzten Rationalitäts-Bereich $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$ angehören. Die Classe der algebraischen Grössen und Gleichungen wird daher ebenso wie die Gattung und Ordnung durch den angenommenen Rationalitäts-Bereich bedingt. Ist aber dieser Bereich festgesetzt, so wird die Classe durch eine *wesentliche*, bei allen rationalen Transformationen von x bleibende, besondere Eigenschaft der Gleichung charakterisirt, welche ich desshalb nach einer von *Jacobi*, wenn auch in anderem Sinne, gebrauchten Ausdrucksweise als den *„Affect“* der Gleichung zum Unterschiede von anderen Eigenschaften derselben bezeichne. Eine irreductible Gleichung

$$(A) \qquad x^n - c_1 x^{n-1} + c_2 x^{n-2} - \cdots \pm c_n = 0,$$

deren Coefficienten c dem Rationalitäts-Bereich $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$ angehören, hat also einen besonderen Affect, wenn eine bestimmte Gattung von Functionen ihrer Wurzeln, welche die „Affect-Gattung“ heissen soll, ebenfalls dem festgesetzten Rationalitäts-Bereich angehört. Die Gruppe der Permutationen der Affect-Gattung ist die *Galois*sche „Gruppe der Gleichung“. Wird

die Affect-Gattung durch $\mathfrak{g}(x_1, x_2, \dots x_n)$ repräsentirt, so ist es das System der $n+1$ Gleichungen

$$(\bar{B}) \qquad \mathfrak{g}(\xi_1, \xi_2, \dots \xi_n) = c_0, \quad \mathfrak{f}_k(\xi_1, \xi_2, \dots \xi_n) = c_k \qquad {\scriptstyle (k=1,2,\dots n)},$$

welches nach dem *Galois*schen Princip an die Stelle der einen Gleichung (A) tritt, und wenn $x_1, x_2, \dots x_n$ als die Unbekannten eines Gleichungssystems aufgefasst werden, so ist das System der n Gleichungen

$$(\bar{C}) \qquad \mathfrak{g}(x_1, x_2, \dots x_n) = c_0, \quad \mathfrak{f}_k(x_1, x_2, \dots x_n) = c_k \qquad {\scriptstyle (k=1,2,\dots n)}$$

so beschaffen, dass es nur durch die r Werthsysteme

$$x_1 = \xi_{r_1}, \quad x_2 = \xi_{r_2}, \quad \dots \quad x_n = \xi_{r_n}$$

befriedigt wird, welche durch die r Permutationen $(r_1, r_2, \dots r_n)$ der Gattung $\mathfrak{g}$ charakterisirt sind. Es ist also von der Ordnung r und bildet den irreductibeln Theil des oben mit (C) bezeichneten Gleichungssystems

$$\mathfrak{f}_k(x_1, x_2, \dots x_n) = c_k \qquad {\scriptstyle (k=1,2,\dots n)},$$

welches von der Ordnung $n!$ ist. Die Zahl r soll auch die Ordnung des Affects und der durch denselben bestimmten Classe genannt werden. Alsdann

> gehört also — immer bei festgesetztem Rationalitäts-Bereich — eine algebraische Grösse n^{ter} Ordnung und die Gleichung, durch welche sie definirt wird, in eine bestimmte Classe der Ordnung r, wenn das Gleichungssystem, durch welches die n conjugirten algebraischen Grössen zugleich definirt werden, von der Ordnung r und durch $n+1$ Gleichungen $(\bar{C})$ darstellbar ist, von denen die erste eine Function einer besonderen für die Classe bestimmenden Gattung, jede der übrigen n aber nur je eine der elementaren symmetrischen Functionen enthält.

Dass, wie hier entwickelt worden ist, jeder irreductible Theil eines Gleichungssystems, welches n conjugirte algebraische Grössen definirt, durch $n+1$ Gleichungen, und zwar — mit Ausnahme des Falles, wo die Ordnung $n!$ ist — nicht durch weniger Gleichungen dargestellt werden kann, fällt unter den allgemeinen für beliebige Gleichungssysteme geltenden Satz, welcher im vorhergehenden Paragraphen aufgestellt worden ist. Aber es bildet eine höchst bemerkenswerthe Eigenthümlichkeit dieser $n+1$ Gleichungen, dass sie auf jene, so zu sagen, „separirte Form“ $(\bar{C})$ gebracht werden können, bei welcher die einen Seiten der Gleichungen nur ganze ganzzahlige, von den gegebenen Grössen $\mathfrak{R}$ unabhängige Functionen der

Unbekannten, die anderen Seiten lediglich rationale Functionen der Grössen $\mathfrak{R}$ enthalten.

An die eigenthümliche „separirte Form" der Gleichungen $(\bar{C})$ lässt sich die Darlegung des principiellen Unterschiedes der *Abel*schen und *Galois*schen Behandlung der algebraischen Gleichungen am besten anknüpfen. *Abel* bleibt nämlich bei den durch die specielle Gleichung gegebenen oder zu ermittelnden rationalen Functionen $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots$ stehen, welche in dem Systeme $(\bar{C})$ die rechte Seite bilden, während *Galois*, wenigstens implicite durch die Aufstellung der Gruppe, von dem speciellen Gleichungsproblem die theoretisch allein wichtigen Functionen auf der linken Seite des Systems $(\bar{C})$ abstrahirt. Freilich entgeht *Galois* eben durch diese vollständige Abstraction auch eines der interessantesten Probleme, welches *Abel* in der Theorie der algebraischen Gleichung findet und auch behandelt. Es ist das Problem der Aufstellung aller Gleichungen einer bestimmten Classe für einen gegebenen Rationalitäts-Bereich, und ich will dasselbe hier auch desshalb näher darlegen, weil dabei die arithmetische Natur algebraischer Fragen deutlich hervortritt.

Wenn mit $\mathfrak{g}$, wie oben, eine Function einer Gattung ϱ^{ter} Ordnung bezeichnet wird, so besteht zwischen $\mathfrak{g}$ und den elementaren symmetrischen Functionen $\mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n$ eine Gleichung

$$\Phi(\mathfrak{g}, \mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n) = 0,$$

in welcher Φ eine ganze ganzzahlige Function der $n+1$ Grössen $\mathfrak{g}, \mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n$ bedeutet, die in Bezug auf $\mathfrak{g}$ vom Grade ϱ ist. Soll es nun für einen Rationalitäts-Bereich $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$ Gleichungen einer durch die Gattung $\mathfrak{g}$ bestimmten Classe geben, so müssen $n+1$ rationale Functionen der Grössen $\mathfrak{R}$

$$\varphi_0, \quad \varphi_1, \quad \varphi_2, \quad \ldots \quad \varphi_n$$

existiren, für welche die Gleichung

$$\Phi(\varphi_0, \varphi_1, \varphi_2, \ldots \varphi_n) = 0$$

erfüllt wird. Die Aufgabe, alle Gleichungen eines bestimmten Affects aufzustellen, ist hiernach durchaus arithmetischer Art, sie ist eine sogenannte Diophantische Aufgabe für den gegebenen Rationalitäts-Bereich, die freilich ebenso schwierig wie interessant zu sein scheint. Selbst für den einfachsten Fall, wo $\mathfrak{g}$ eine alternirende Function bedeutet, ist die Aufgabe für ein allgemeines n, so viel ich weiss, noch nicht gelöst worden. In diesem Falle

ist der Grad von Φ in Bezug auf $\mathfrak{g}$ möglichst klein, nur gleich *Zwei;* die Schwierigkeit der Aufgabe scheint aber nicht mit der Grösse des Grades zu wachsen; denn für den Fall, wo $\mathfrak{g}$ eine cyclische Function darstellt, und also jener Grad so gross als möglich ist, habe ich die Lösung schon in meiner oben citirten Mittheilung vom Juni 1853 gegeben. Damals hatte ich allerdings für allgemeine Rationalitäts-Bereiche den Fall, wo n eine Potenz von *Zwei* ist, noch ausschliessen müssen, ich habe aber später auch diesen Fall erledigt und dabei gefunden, dass die Aufgabe in der That für $n = 8, 16, 32, \ldots$ einen ganz anderen Charakter hat als für die übrigen Zahlen n.

Da die ganzen rationalen Functionen $x_1, x_2, \ldots x_n$ als algebraische Functionen von $\mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n$ aufgefasst werden können und als solche eben jene Gattungen bilden, welche zur Definition der Functions-Gattungen gedient haben, so müssen alle zu einer Gattung gehörigen ganzen Functionen, welche also die Haupt-Art bilden, gemäss § 6 durch eine bestimmte Anzahl von Elementen linear darstellbar sein, und es ist schon in § 7 erwähnt, dass die ausreichende Anzahl in diesem Falle nicht grösser ist als die Ordnung der Gattung. Ich habe diesen Fundamentalsatz zuerst in meinen im Winter 1870/71 gehaltenen Universitäts-Vorlesungen vorgetragen und will hier die damals gegebene Entwickelung in Kürze mittheilen.

Das Fundamentalsystem für die *Galois*sche Gattung kann durch die $n!$ Elemente

$$x_1^{h_1} x_2^{h_2} \ldots x_{n-1}^{h_{n-1}} \qquad (h_k = 0, 1, \ldots n-k;\ k = 1, 2, \ldots n-1)$$

dargestellt werden. Ich habe dies zuerst in meinem schon oben citirten Aufsatz „Ueber die verschiedenen *Sturm*schen Reihen" im Monatsbericht der Berliner Akademie vom Febr. 1873 nachgewiesen. Da nämlich das Product

$$(x - x_k)(x - x_{k+1}) \ldots (x - x_n)$$

für jeden der n Werthe $k = 1, 2, \ldots n$ eine ganze Function $(n-k+1)^{\text{ten}}$ Grades von x ist, deren Coefficienten ganze ganzzahlige Functionen von

$$x_1, \quad x_2, \quad \ldots \quad x_{k-1}; \quad \mathfrak{f}_1, \quad \mathfrak{f}_2, \quad \ldots \quad \mathfrak{f}_n$$

sind, so stellt dasselbe, gleich Null gesetzt, eine Gleichung für x_k dar, mit deren Hülfe sich jede höhere als die $(n-k)^{\text{te}}$ Potenz von x_k durch niedrigere so ausdrücken lässt, dass die Coefficienten ganze ganzzahlige Functionen von $x_1, x_2, \ldots x_{k-1}$ und $\mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n$ werden. Indem man dies nun der Reihe nach für $k = n,\ n-1,\ n-2, \ldots$ ausführt, kann man jede ganzzahlige

Function von $x_1, x_2, \dots x_n$ auf eine solche reduciren, welche in Beziehung auf jedes x_k nur vom Grade $n-k$ ist, und deren Coefficienten ganze ganzzahlige Functionen der elementaren symmetrischen Functionen $\mathfrak{f}$ sind. Eine solche „reducirte Form" einer ganzen Function von $x_1, x_2, \dots x_n$ ist offenbar völlig bestimmt und eben nichts Anderes als die Darstellung durch das angegebene Fundamentalsystem der *Galois*schen Gattung. Dabei ergiebt sich übrigens in einfachster, naturgemässer Weise die Darstellbarkeit jeder ganzen symmetrischen Function von $x_1, x_2, \dots x_n$ als ganze ganzzahlige Function von $\mathfrak{f}_1, \mathfrak{f}_2, \dots \mathfrak{f}_n$.

Denkt man sich die obigen Elemente eines Fundamentalsystems der *Galois*schen Gattung nach ihrer Dimension geordnet, diejenigen von gleicher Dimension aber in je eine Gruppe vereinigt, und bezeichnet man dieselben der Reihe nach mit $\gamma', \gamma'', \gamma''', \dots$, so kann man entsprechende ganze Functionen einer gegebenen Gattung $\mathfrak{g}', \mathfrak{g}'', \mathfrak{g}''', \dots$ daraus bilden, indem man diejenigen aus einem Element γ durch die r Permutationen der Gattung entstehenden Functionen, welche unter einander verschieden sind, zu einander addirt. Dann lässt sich offenbar jede ganze Function der Gattung $\mathfrak{g}$ als lineare ganze Function von $\mathfrak{g}', \mathfrak{g}'', \mathfrak{g}''', \dots$ so darstellen, dass die Coefficienten ganze ganzzahlige Functionen von $\mathfrak{f}_1, \mathfrak{f}_2, \dots \mathfrak{f}_n$ sind; die $n!$ Elemente bilden also im vollen Sinne des Wortes ein Fundamentalsystem der Gattung $\mathfrak{g}$. Es soll aber nunmehr nachgewiesen werden, dass sich alle diese $n!$ Elemente durch nur ϱ derselben linear darstellen lassen, wenn man als Coefficienten ganze Functionen von $\mathfrak{f}_1, \mathfrak{f}_2, \dots \mathfrak{f}_n$ mit bloss rationalen, d. h. auch mit gebrochenen Zahlcoefficienten zulässt, dass also für ein Fundamentalsystem in diesem nicht ganz vollen Sinne des Wortes eine die Ordnungszahl ϱ nicht übersteigende Anzahl von Elementen genügt (vgl. den Anfang des § 7).

Bei jeder Darstellung einer Function $\mathfrak{g}$ durch die Functionen γ

$$(\Gamma) \qquad \mathfrak{g}^{(k)} = \varphi'_k \gamma' + \varphi''_k \gamma'' + \varphi'''_k \gamma''' + \cdots,$$

wobei $\varphi'_k, \varphi''_k, \varphi'''_k, \dots$ ganze ganzzahlige Functionen von $\mathfrak{f}_1, \mathfrak{f}_2, \dots \mathfrak{f}_n$ bedeuten, können nur Functionen γ von der durch $\mathfrak{g}$ selbst repräsentirten oder von voranstehenden Gruppen vorkommen. Addirt man alle diejenigen Gleichungen (Γ), welche bei den r Permutationen der Gattung daraus entstehen, zu einander, so resultirt eine Gleichung

$$(G) \qquad r\mathfrak{g}^{(k)} = m'\varphi'_k \mathfrak{g}' + m''\varphi''_k \mathfrak{g}'' + m'''\varphi'''_k \mathfrak{g}''' + \cdots,$$

in welcher $m', m'', m''', \dots$ ganze Zahlen und zwar Theiler von r bedeuten,

da $\Sigma\gamma$, wenn in Beziehung auf alle r Permutationen summirt wird, die entsprechende Function $\mathfrak{g}$ mehrmals ergiebt. Die Gleichung (G) zeigt, dass alle diejenigen Functionen $\mathfrak{g}^{(k)}$, bei deren Darstellung (Γ) durch die Elemente γ nur solche von voranstehenden Gruppen vorkommen, sich zugleich auf lineare Functionen von ***Gattungs-Elementen*** $\mathfrak{g}$ der voranstehenden Gruppen reduciren. Die Coefficienten dieser linearen Functionen sind ganze Functionen von $\mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n$ mit rationalen Zahlcoefficienten. Alle auf die angegebene Weise reducirbaren Elemente $\mathfrak{g}$ können also weggelassen werden, und es bleiben dann nur solche Functionen $\mathfrak{g}^{(k)}$ übrig, welche bei der Darstellung (Γ) auch Elemente γ von derselben Gruppe wie die dargestellte Function $\mathfrak{g}$ und zwar diese mit ganzzahligen Coefficienten enthalten. Bezeichnet man diese linearen Aggregate von Elementen γ der höchsten Dimension, welche nur ganzzahlige Coefficienten haben, mit $\Gamma^{(k)}$, so ist $\mathfrak{g}^{(k)} - \Gamma^{(k)}$ eine Function, welche bei ihrer Darstellung durch die Elemente γ nur solche von geringerer Dimension enthält. Nimmt man nun die einzelnen Functionen $\mathfrak{g}^{(k)}$, welche einer und derselben Gruppe angehören, in einer beliebigen Reihenfolge, so lässt sich, wenn eines der Aggregate $\Gamma^{(k)}$ durch Aggregate $\Gamma^{(k-1)}, \Gamma^{(k-2)}, \ldots$ von voranstehenden Elementen $\mathfrak{g}^{(k-1)}, \mathfrak{g}^{(k-2)}, \ldots$ linear darstellbar ist, das Element $\mathfrak{g}^{(k)}$ selbst als eine lineare Function voranstehender Elemente $\mathfrak{g}^{(k-1)}, \mathfrak{g}^{(k-2)}, \ldots$ ausdrücken. Ist nämlich

$$\Gamma^{(k)} = c_1 \Gamma^{(k-1)} + c_2 \Gamma^{(k-2)} + \cdots,$$

so wird

$$\begin{aligned} \mathfrak{g}^{(k)} &= c' \mathfrak{g}^{(k-1)} + c'' \mathfrak{g}^{(k-2)} + \cdots + (\mathfrak{g}^{(k)} - \Gamma^{(k)}) \\ &\quad - c'(\mathfrak{g}^{(k-1)} - \Gamma^{(k-1)}) - c''(\mathfrak{g}^{(k-2)} - \Gamma^{(k-2)}) - \cdots, \end{aligned}$$

und ebenso, wie jedes einzelne Glied $\mathfrak{g} - \Gamma$, enthält der ganze zweite Theil auf der rechten Seite dieser Gleichung bei der Darstellung durch die Elemente γ nur solche von geringerer Dimension als $\mathfrak{g}^{(k)}$, und erfüllt daher, als Function der Gattung $\mathfrak{g}$, diejenigen Bedingungen, für welche oben nachgewiesen worden, dass sich eine solche Function linear durch Gattungselemente $\mathfrak{g}$ von geringerer Dimension darstellen lässt. Nach Weglassung aller solcher Elemente $\mathfrak{g}^{(k)}$, deren zugehörige Aggregate $\Gamma^{(k)}$ durch Aggregate voranstehender linear ausdrückbar sind, bleiben nur Elemente $\mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g}_3, \cdots$ übrig, welche in dem Sinne linear unabhängig von einander sind, dass keine Relation

$$\psi_1 \mathfrak{g}_1 + \psi_2 \mathfrak{g}_2 + \psi_3 \mathfrak{g}_3 + \cdots = 0$$

besteht, in welcher $\psi_1, \psi_2, \psi_3, \ldots$ ganze Functionen von $\mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n$ sind. Denn schon zwischen den entsprechenden Aggregaten der höchsten Dimension $\Gamma_1, \Gamma_2, \Gamma_3, \ldots$ kann keine lineare Relation mit Coefficienten ψ bestehen. Die Anzahl der übrig gebliebenen Functionen $\mathfrak{g}$ muss demnach genau gleich ϱ sein, da dies die Anzahl der von einander linear unabhängigen Functionen der Gattung $\mathfrak{g}$ ist.

Wird die Discriminante der durch x_k bezeichneten Gattung, nämlich das Product

$$\Pi(x_i - x_k) \qquad (i, k = 1, 2, \ldots n;\ i \gtrless k)$$

mit $\mathfrak{D}$ bezeichnet, so ist die Discriminante der *Galois*schen Gattung $\mathfrak{D}^{\frac{1}{2}n!}$. Nach § 8 ist also auch die Discriminante jeder anderen Gattung eine Potenz von $\mathfrak{D}$. Denn jede solche Gattung ist unter der *Galois*schen enthalten; ihre Discriminante muss daher Theiler einer Potenz von $\mathfrak{D}$ und also, da $\mathfrak{D}$ im Rationalitäts-Bereich $(\mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n)$ irreductibel ist, selbst eine Potenz von $\mathfrak{D}$ sein.

Bedeuten $\mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g}_3, \ldots$ ganze ganzzahlige Functionen von $x_1, x_2, \ldots x_n$, welche der Gattung $\mathfrak{g}$ angehören, und in dem oben angegebenen Sinne ein Fundamentalsystem dieser Gattung bilden, so kann nach § 8 die Discriminante der Gleichung, welcher

$$u_1\mathfrak{g}_1 + u_2\mathfrak{g}_2 + u_3\mathfrak{g}_3 + \cdots$$

genügt, keinen anderen von den unbestimmten Grössen u unabhängigen Factor enthalten als einen solchen, der Theiler einer Potenz der Discriminante der Gattung $\mathfrak{g}$ ist; es kann daher, wenn jene Discriminante nach Producten von Potenzen der unbestimmten Grössen u entwickelt wird, der grösste gemeinsame Theiler sämmtlicher dabei auftretender Coefficienten nur eine Potenz von $\mathfrak{D}$ sein. Hieraus folgt, dass sich für irgend welche gegebenen Werthe von $\mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n$ — vorausgesetzt nur, dass der Werth von $\mathfrak{D}$ dafür nicht verschwindet — stets unendlich viele specielle Functionen jeder Gattung $\mathfrak{g}$ bestimmen lassen, deren sämmtliche conjugirte unter einander verschieden sind, und durch die sich daher jede andere Function derselben Gattung rational ausdrücken lässt.

§ 13.

Begründung der arithmetischen Existenz der algebraischen Grössen.

Die am Schlusse des vorigen Paragraphen entwickelte Eigenschaft der Gattungen algebraischer Functionen von $\mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n$ bildet die wesentlichste Grundlage bei einem dem *Gauss*schen Beweise von 1815 nachge-

bildeten Existenzbeweise für die Wurzeln algebraischer Gleichungen, welchen ich schon in meiner an der hiesigen Universität gehaltenen Wintervorlesung von 1870/71 vorgetragen und seitdem in meinen Vorlesungen über die Theorie der algebraischen Gleichungen stets fast in derselben Weise gegeben habe. — Der Beweis stützt sich auf „uneigentliche“ Functionsgattungen, welche entstehen, wenn man aus einer Gattung $\mathfrak{g}(x_1, x_2, \dots x_h)$, falls $h < \frac{1}{2}n$ ist, eine neue bildet, die durch

$$(z-\mathfrak{g}(x_1, x_2, \dots x_h))(z-\mathfrak{g}(x_{h+1}, x_{h+2}, \dots x_{2h}))$$

repräsentirt wird. Nimmt man nämlich nach einander $h = 1, 2, 4, \dots 2^\nu$, und bezeichnet die entsprechenden Gattungen mit $\mathfrak{g}_0, \mathfrak{g}_1, \mathfrak{g}_2, \dots \mathfrak{g}_\nu$, so enthält die Zahl, welche die Ordnung der Gattung $\mathfrak{g}_\mu$ angiebt, genau die $(\nu-\mu)^{\text{te}}$ Potenz von 2, wenn die Zahl n keine höhere als die ν^{te} Potenz von 2 enthält. Die Ordnung von $\mathfrak{g}_\nu$ ist also ungrade. Es ist ferner $\mathfrak{g}_{\mu-1}$ Wurzel einer quadratischen Gleichung, deren Coefficienten der Gattung $\mathfrak{g}_\mu$ angehören, so dass

$$\mathfrak{g}_{\mu-1} = \varphi(\mathfrak{g}_\mu) + \sqrt{\psi(\mathfrak{g}_\mu)}$$

wird. Hierbei bedeuten φ und ψ ganze Functionen von $\mathfrak{g}_\mu$, deren Coefficienten rationale Functionen von $\mathfrak{f}_1, \mathfrak{f}_2, \dots \mathfrak{f}_n$ sind, und es kann darin nur die Discriminante der Gleichung, welcher die als Repräsentant der Gattung gewählte, bestimmte Function $\mathfrak{g}_\mu$ genügt, oder ein Theiler derselben als Nenner vorkommen. Die Kette jener Gleichungen für $\mu = 1, 2, \dots \nu$ giebt hiernach $\mathfrak{g}_0$ oder, was dafür genommen werden kann, x_1 als explicite, lediglich Quadratwurzeln enthaltende, ganze algebraische Function von $\mathfrak{g}_\nu$ und $\mathfrak{f}_1, \mathfrak{f}_2, \dots \mathfrak{f}_n$, dividirt durch eine ganze Function von $\mathfrak{f}_1, \mathfrak{f}_2, \dots \mathfrak{f}_n$, welche nur ein Theiler des Products gewisser Discriminanten sein kann. Wird dieses Product mit $\mathfrak{p}$ bezeichnet, so existirt daher eine lediglich durch Quadratwurzeln aus ganzen ganzzahligen Functionen von $y, \mathfrak{f}_1, \mathfrak{f}_2, \dots \mathfrak{f}_n$ zu bildende algebraische Function $\theta(y)$, welche, wenn darin $y = \mathfrak{g}_\nu$ genommen wird, $\mathfrak{p}x_1$ ergiebt. Die algebraische Function $\theta(y)$ ist von der Ordnung 2^ν; es besteht daher eine Gleichung $\mathfrak{P}(x, y) = 0$ des Grades 2^ν, welche durch den Werth $x = \frac{\theta(y)}{\mathfrak{p}}$ befriedigt wird, und, wenn der Coefficient der höchsten Potenz von x gleich Eins ist, in ihren übrigen Coefficienten nur ganze Functionen von $y, \mathfrak{f}_1, \mathfrak{f}_2, \dots \mathfrak{f}_n$, dividirt durch Potenzen von $\mathfrak{p}$, enthält. Nun ist

$$\prod_h (x-x_h) = \mathfrak{P}(x, \mathfrak{g}_\nu) \qquad (h=1,2,3,\dots 2^\nu)$$

und folglich

$$\mathfrak{F}(x) = \mathfrak{P}(x, \mathfrak{g}_\nu)\mathfrak{Q}(x, \mathfrak{g}_\nu),$$

wo auch $\mathfrak{Q}$ ganz ebenso wie $\mathfrak{P}$ eine ganze Function von x, $\mathfrak{g}_\nu$ bedeutet, deren Coefficienten rationale, nur Potenzen von $\mathfrak{p}$ im Nenner enthaltende Functionen der Grössen $\mathfrak{f}$ sind. Wenn also $\mathfrak{G}(y) = 0$ die Gleichung ist, durch welche $\mathfrak{g}_\nu$ als algebraische Function der Grössen $\mathfrak{f}$ definirt wird, so muss eine identische Gleichung

$$\mathfrak{F}(x) = \mathfrak{P}(x, y)\mathfrak{Q}(x, y) + \mathfrak{G}(y)\mathfrak{R}(x, y)$$

bestehen, in welcher auch $\mathfrak{R}(x, y)$ eine Function von derselben Beschaffenheit wie $\mathfrak{P}$ und $\mathfrak{Q}$ bedeutet. Setzt man hierin $x = \frac{\theta(y)}{\mathfrak{p}}$, so wird $\mathfrak{P}(x,y) = 0$, und es resultirt die identische, d. h. für jeden beliebigen Werth von y geltende Gleichung

$$\mathfrak{F}\left(\frac{\theta(y)}{\mathfrak{p}}\right) = \mathfrak{G}(y)\mathfrak{R}\left(\frac{\theta(y)}{\mathfrak{p}}, y\right),$$

welche zeigt, dass die Gleichung $\mathfrak{F}(x) = 0$ durch die algebraische Grösse $\frac{\theta(y)}{\mathfrak{p}}$ befriedigt wird, wenn y der Gleichung $\mathfrak{G}(y) = 0$ genügt und $\mathfrak{p}$ nicht verschwindet. Da nun am Ende des vorigen Paragraphen der diesen letzten Schluss einzig ermöglichende Nachweis geführt ist, dass für solche Werthe von $\mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n$, für welche die Discriminante der Gleichung $\mathfrak{F}(x) = 0$ von Null verschieden ist, stets die Functionen $\mathfrak{g}_1, \mathfrak{g}_2, \ldots \mathfrak{g}_n$ so gewählt werden können, dass jede der betreffenden Discriminanten und also auch deren Product $\mathfrak{p}$ einen von Null verschiedenen Werth hat, so folgt, dass jeder Gleichung durch eine explicite algebraische, nur Quadratwurzeln enthaltende Function einer Grösse y genügt wird, welche selbst Wurzel einer Gleichung ungraden Grades ist.

Es verdient hervorgehoben zu werden, dass in dieser Entwickelung, wie in der citirten *Gauss*schen Abhandlung von 1815, eine viel *speciellere* Art der Existenz algebraischer Grössen dargelegt wird, als bei allen anderen Beweismethoden. Dieser Unterschied tritt besonders deutlich hervor, wenn man den oben für Gleichungen ungraden Grades vorausgesetzten Begriff der reellen Wurzeln algebraischer Gleichungen genauer analysirt, wie ich es in meinen Universitäts-Vorlesungen regelmässig gethan habe; und ich gedenke auch diese Analyse bei einer nächsten Gelegenheit durch den Druck zu veröffentlichen. Der hier entwickelte Beweis enthält recht eigentlich eine Begründung der *arithmetischen* Existenz der algebraischen Grössen und fügt sich desshalb in die systematische Darstellung, welche ich in der vorliegenden Arbeit zu geben versucht habe, vollständig ein.

Zweiter Theil.

§ 14.

Die grössten gemeinschaftlichen Theiler von ganzen algebraischen Grössen.

Mit dem Begriffe der ganzen algebraischen Grössen (vgl. § 5) ist der Begriff der Theilbarkeit unmittelbar gegeben. Eine ganze algebraische Grösse x ist durch eine andere x' theilbar, wenn der Quotient der Division von x durch x' wiederum eine ganze algebraische Grösse ist. Hierbei ist der Divisor x' als gegeben zu betrachten. Aber auch die andere Frage der Auffindung oder Aufstellung der Divisoren gegebener algebraischer Grössen lässt eine höchst einfache Behandlung zu. In der That hat man zu den algebraischen Grössen einer bestimmten Art oder Species $\mathfrak{S}$ nur *lineare Functionen derselben mit unbestimmten Coefficienten* hinzu zu nehmen, um ohne alle Symbolik und ohne alle Mittel der Abstraction die grössten gemeinsamen Theiler je zweier algebraischer Grössen der gesammten Art $\mathfrak{S}$ wirklich darzustellen. Bedeuten nämlich $u', u'', \ldots$ unbestimmte Grössen und $x, x', x'', \ldots$ ganze algebraische Grössen einer bestimmten Art $\mathfrak{S}$, so ist das über alle conjugirten Werthe erstreckte Product

$$\Pi(x+u'x'+u''x''+\cdots),$$

welches auch nach der üblichen Ausdrucksweise als die „Norm" von $x+u'x'+u''x''+\cdots$ und demnach mit

$$\mathrm{Nm}(x+u'x'+u''x''+\cdots)$$

bezeichnet werden kann, eine ganze Function der Grössen u, deren Coefficienten ganze rationale Grössen des Bereichs sind. Wird nun zunächst — wie unbeschadet der Allgemeinheit geschehen kann — von dem Falle abstrahirt, wo nicht sämmtliche Grössen $\mathfrak{R}$ von einander unabhängig sind, wird also ein natürlicher Rationalitätsbereich angenommen, so ist der Begriff des grössten gemeinsamen Theilers aller jener Coefficienten ohne Weiteres begründet, da diese Coefficienten alsdann nur ganze Zahlen oder ganze ganzzahlige Functionen unabhängiger Veränderlicher sind. Eben derselbe Theiler kann auch als der grösste von den Unbestimmten u unabhängige Theiler der Norm von $x+u'x'+u''x''+\cdots$ charakterisirt werden, und der nach Absonderung dieses Theilers verbleibende Theil der Norm ist eine ganze

Function von u', u'', ..., deren Coefficienten ganze rationale Grössen des Bereichs sind, die nicht sämmtlich einen und denselben gemeinsamen Theiler haben. Nennt man diese ganze Function, obwohl sie nicht homogen ist, doch in *Gauss*scher Weise eine in Linearfactoren zerlegbare *„primitive Form n^{ten} Grades von u', u'', ...“*, deren *„abgeleitete“* die Norm von $x+u'x'+u''x''+\cdots$ ist, und bezeichnet dieselbe mit

$$\mathrm{Fm}(x+u'x'+u''x''+\cdots),$$

so besteht, der Definition gemäss, zwischen der „Norm“ und der „Form“ eine Relation

$$P.\mathrm{Fm}(x+u'x'+u''x''+\cdots) = \mathrm{Nm}(x+u'x'+u''x''+\cdots),$$

in welcher P eine ganze rationale Grösse des Bereichs ist. Dies vorausgeschickt, kann *„der grösste gemeinschaftliche Theiler“* beliebig vieler ganzer algebraischer Grössen x, x', x'', ... durch den Bruch

$$\frac{x+u'x'+u''x''+\cdots}{\mathrm{Fm}(x+u'x'+u''x''+\cdots)}$$

vollkommen dargestellt werden, da jede lineare Function $x+v'x'+v''x''+\cdots$ mit beliebigen Coefficienten v durch jenen Bruch theilbar ist, der Quotient der Division aber keinen solchen Bruch mehr als Theiler enthalten kann. Um das Erstere einzusehen, braucht man nur die Gleichung zu bilden, welcher der Quotient

$$\frac{x+v'x'+v''x''+\cdots}{x+u'x'+u''x''+\cdots}\cdot\mathrm{Fm}(x+u'x'+u''x''+\cdots)$$

genügt, d. h. also, wenn dieser Quotient mit $Q(x, x', x'', \ldots)$ bezeichnet wird, die Gleichung

$$\mathrm{Nm}(X-Q(x, x', x'', \ldots)) = 0,$$

in welcher X die Unbekannte bedeutet. Die Norm auf der linken Seite der Gleichung nimmt nämlich, wenn zur Abkürzung erst

$$\mathrm{Fm}(x+u'x'+u''x''+\cdots) \doteq F$$

und dann

$$X-F=w,\quad u'X-v'F=w',\quad u''X-v''F=w'', \ldots$$

gesetzt wird, die Gestalt an

$$\frac{\mathrm{Fm}(wx+w'x'+w''x''+\cdots)}{\mathrm{Fm}(x+u'x'+u''x''+\cdots)},$$

und es wird hiermit evident, dass dieser Ausdruck eine ganze ganzzahlige

Function der Grössen X, $\mathfrak{R}'$, $\mathfrak{R}''$, $\mathfrak{R}'''$, $\ldots$, u', u'', $\ldots$ v', v'', $\ldots$ ist, welcher überdies als Coefficienten der höchsten Potenz von X die Zahl Eins und also, gleich Null gesetzt, *ganze* algebraische Grössen zu Wurzeln hat. Dass nun zweitens der mit $Q(x, x', x'', \ldots)$ bezeichnete Quotient nicht noch durch einen Bruch

$$\frac{x_1 + u_1' x_1' + u_1'' x_1'' + \cdots}{\mathrm{Fm}(x_1 + u_1' x_1' + u_1'' x_1'' + \cdots)}$$

theilbar sein kann, erhellt unmittelbar, wenn man nach erfolgter Division die Norm bildet. Diese Norm wird nämlich, wenn

$$P_1 . \mathrm{Fm}(x_1 + u_1' x_1' + u_1'' x_1'' + \cdots) = \mathrm{Nm}(x_1 + u_1' x_1' + u_1'' x_1'' + \cdots)$$

ist, gleich

$$\frac{1}{P_1} \mathrm{Fm}(x + v'x' + v''x'' + \cdots) . (\mathrm{Fm}(x + u'x' + u''x'' + \cdots) . \mathrm{Fm}(x_1 + u_1' x_1' + u_1'' x_1'' + \cdots))^{n-1},$$

also nur dann ganz, wenn $P_1 = 1$ ist.

Dass die Divisoren der ganzen algebraischen Grössen in Bruchform dargestellt sind, kann keinen Anstoss erregen; denn die Uebertragung des ursprünglichsten Begriffes der Division mit ganzen Zahlen auf die mit gebrochenen gehört schon den Elementen an. *Complexe* gebrochene Zahlen habe ich als Moduln oder Divisoren zuerst in § 6 meiner Doctordissertation „De unitatibus complexis“ (Berlin 1845) genau so angewendet, wie sie wenige Jahre darauf in der *Kummer*schen Definition der idealen Zahlen benutzt werden (vgl. die Anmerk. in § 19), und sie haben namentlich auch in den *Exponenten* der Einheiten wesentliche Dienste geleistet. Aber erst viel später wurde ich beim Uebergang von den complexen Zahlen zu den zerlegbaren Formen (vgl. § 19) darauf geführt, das Hülfsmittel der gebrochenen Divisoren mit jenem „methodischen Hülfsmittel der unbestimmten Coefficienten“ combinirt anzuwenden, um alle unnützen und theilweise auch verwirrenden Specialitäten abzustreifen. Damit erschienen dann in der That die Divisoren der ganzen algebraischen Grössen in einfacher, übersichtlicher, naturgemässer Gestalt, in welcher für den speciellen Fall der gewöhnlichen Zahlen, d. h. für den Fall $\mathfrak{R} = 1$, alle sowohl bei der *Kummer*schen Begriffsbestimmung der idealen Zahlen als auch bei der *Dedekind*schen Definition der „Ideale“ benutzten abstracten Eigenschaften an einem concreten algebraischen Gebilde vereinigt sind. Der Grund dieses Erfolges liegt einfach darin, dass mit jenen Divisoren das Gebiet der algebraischen Grössen, welche den Ausgangspunkt bilden, genügend erweitert wird, um den bei

ganzen Zahlen und bei ganzen rationalen Functionen von Variabeln geltenden einfachen Gesetzen der Theilbarkeit, welche beim Uebergang zu den ganzen algebraischen Grössen modificirt werden, wiederum Raum zur vollen Wirksamkeit zu schaffen. Es ist also ein von den bisher angewendeten Methoden principiell verschiedenes Verfahren, welches ich bei Einführung jener Divisoren eingeschlagen habe, es ist das *„Princip der Association neuer Grössengebilde zu der gegebenen Gattung und Species algebraischer Grössen“*, welches hierbei die Grundlage bildet*).

§ 15.

Die algebraischen Divisoren.

Eine ganze algebraische Grösse, deren Norm gleich Eins und durch welche also jede ganze algebraische Grösse theilbar ist, soll eine „algebraische Einheit“ genannt werden. Diese Einheiten sind durch keine anderen ganzen algebraischen Grössen theilbar. Ebendieselbe Eigenschaft besitzen auch die „primitiven Formen“, welche die Nenner jener „Divisoren ganzer algebraischer Grössen“ bilden, und es könnten desshalb die Zähler allein schon als Repräsentanten der Divisoren gebraucht werden, wenn bei den Quotienten der Division von solchen Nennern, die durch keine ganze algebraische Grösse theilbar sind, abgesehen wird. Diese Betrachtungsweise wird später (in § 22) systematisch angewendet werden; hier im Anfang der Entwickelung glaube ich der obigen Darstellung der Divisoren den Vorzug geben zu sollen, weil sie *keinerlei* Abstraction erfordert. Nur eine der Sache entsprechende abgekürzte Ausdrucks- und Bezeichnungsweise einzuführen erscheint wohl statthaft. Um nämlich nicht jedes Mal für die *Form* eines linearen Ausdrucks $x+u'x'+u''x''+\cdots$ ein besonderes Zeichen zu benutzen, soll unter dem „Modul $[x+u'x'+u''x''+\cdots]$“ oder „dem Divisor $[x+u'x'+u''x''+\cdots]$“ der lineare Ausdruck selbst, dividirt durch die daraus entstehende primitive Form, verstanden und mit

$$\operatorname{mod}[x+u'x'+u''x''+\cdots] \quad \text{oder} \quad \operatorname{div}[x+u'x'+u''x''+\cdots]$$

bezeichnet werden. Im Sinne des in dieser Arbeit vielfach benutzten „methodischen Hülfsmittels der unbestimmten Coefficienten“, welches zu der obigen Bildungsweise der Divisoren geführt hat, sind die Ausdrücke $x+u'x'+u''x''+\cdots$

---

*) Vgl. die weiteren Ausführungen über die „Association“ in § 22.

dabei als lineare Functionen der Grössen x mit unbestimmten Coefficienten u bezeichnet worden; doch ist es von allgemeinerem Gesichtspunkte aus geeigneter, die Grössen x als die Coefficienten der Unbestimmten u und also jene algebraischen Ausdrücke als „lineare Formen" mit ganzen algebraischen Coefficienten aufzufassen. Denn ausser den bereits eingeführten, aus *linearen* Formen hervorgegangenen algebraischen Divisoren können noch allgemeinere aus Formen beliebiger Grade gebildet werden, und es ist sogar *nothwendig*, diese mit in den Kreis der Betrachtung zu ziehen, weil bei der Division einer linearen Form durch einen der oben eingeführten Divisoren der Quotient eine ganze Function der Unbestimmten von höherem Grade, also eine „Form" höheren Grades wird.

Zum Zwecke der Definition der allgemeineren Divisoren muss nunmehr die der Formen vorausgeschickt werden.

I. Eine ganze rationale Function beliebig vieler unbestimmter Grössen $u, v, w, \ldots$ soll, wenn die Coefficienten *ganze* Grössen des natürlichen Rationalitäts-Bereichs $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$, also Grössen des in § 5 mit $[\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots]$ bezeichneten Bereichs sind, eine *„ganze" (rationale) Form des Bereichs* $[\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots]$ *mit den Unbestimmten* $u, v, w, \ldots$, und, wenn die Coefficienten ganze algebraische Grössen eines Gattungs-Bereichs $(\mathfrak{G})$ und eines Art-Bereichs $(\mathfrak{S})$ sind und wenigstens einer derselben der Art $\mathfrak{S}$ selbst angehört, eine *„ganze algebraische Form der Gattung* $\mathfrak{G}$ *und der Art* $\mathfrak{S}$*"* genannt werden.

Die ganzen algebraischen Formen, im weiteren Sinne des Wortes, umfassen auch die ganzen rationalen Formen, ebenso wie die ganzen algebraischen Grössen die ganzen rationalen mit umfassen.

II. Enthalten die Formen die Unbestimmten nur linear, so sollen sie als „ganze rationale" oder „ganze algebraische *Linearformen*" bezeichnet werden.

III. Die ganzen rationalen Formen heissen *„primitiv"*, wenn ihre Coefficienten keinen gemeinsamen Theiler haben. Eine ganze algebraische Form ist als primitiv zu bezeichnen, wenn ihre Norm primitiv ist.

Eine weitere Unterscheidung der primitiven Formen in eigentlich und uneigentlich primitive wird später in § 22 gegeben werden.

Die Uebertragung der üblichen Bezeichnung „Form" auf nicht homogene ganze Functionen scheint mir keinem Bedenken zu unterliegen. Das

Zutreffende an der Bezeichnung ist, dass sie, im Gegensatz zur Benennung „*Function* der Grössen u, v, w, ...", die Coefficienten als das Wesentliche, die Unbestimmten als das Unwesentliche kennzeichnet. Da hier, genau so wie im gewöhnlichen Sinne, das Wort „Form" schon an sich einen Ausdruck bedeutet, welcher in Bezug auf die Unbestimmten der Form ganz und rational ist, so konnten in den aufgestellten Definitionen jene Bezeichnungen „ganze rationale", „ganze algebraische" Formen, welche die Natur der *Coefficienten* charakterisiren sollen, unbedenklich als adjectivische den Formen selbst beigelegt werden. Auch die Begriffe des Conjugirt-Seins, der Norm u. s. w. sollen im Folgenden, ebenso wie der Begriff der Gattung und Art, von den *Coefficienten* auf die algebraischen Formen selbst übertragen werden.

IV. Wird eine ganze algebraische Form durch diejenige primitive Form dividirt, deren abgeleitete die Norm der algebraischen Form ist, so repräsentirt der Quotient einen allgemeinen „*algebraischen Modul oder Divisor*", dessen „*Elemente*" durch die Coefficienten der algebraischen Form gebildet werden.

Es verdient hervorgehoben zu werden, dass diese Definition auch für den besonderen Fall Geltung behält, wo die ganze algebraische Form sich auf eine ganze *rationale* reducirt, also die Anzahl der Conjugirten gleich Eins, und die Norm daher mit der ganzen rationalen Form selbst identisch wird.

Nach den gegebenen Definitionen sind die ganzen algebraischen Grössen selbst ebenso in den ganzen algebraischen Formen wie in den algebraischen Divisoren mit inbegriffen, und eben, damit dies der Fall sei, hat die Beschränkung auf homogene Formen aufgegeben werden müssen. Das Verhältniss der ganzen algebraischen Grössen zu den Formen und Divisoren, unter denen sie mit inbegriffen sind, ist in folgender Weise einfach zu charakterisiren:

V. In einer bestimmten Art oder Species bilden die ganzen algebraischen *Grössen* die „Hauptclasse" der algebraischen Divisoren; sie gehören auch zur Hauptclasse der ganzen algebraischen Formen (vgl. § 22, VII), sowie die algebraischen Einheiten gewissermassen die Hauptclasse der *primitiven* algebraischen Formen ausmachen.

Mit Hülfe der obigen Definitionen kann der Begriff der Theilbarkeit der Formen und Divisoren genau und einfach präcisirt werden.

VI. Eine ganze algebraische Form ist durch einen algebraischen Divisor theilbar, wenn der Quotient ebenfalls eine ganze algebraische Form ist.

VII. Ein algebraischer Divisor soll als theilbar durch einen anderen Divisor bezeichnet werden, wenn die Form, welche den Zähler des ersteren bildet, durch den letzteren theilbar ist.

Der hier aufgestellte Begriff der Theilbarkeit ist in der gewöhnlichen Weise nach *Gauss* für den Congruenzbegriff zu benutzen, und es soll auch das *Gauss*sche Congruenzzeichen zuweilen gebraucht werden.

Da die Brüche, welche in der obigen Definition (IV) als algebraische Divisoren definirt sind, nur in ihrer Eigenschaft als Divisoren Anwendung finden, so sind alle diejenigen, welche einander in dieser Eigenschaft vollkommen ersetzen, als äquivalent zu betrachten; und, um dies ausdrücklich zu formuliren, sei hier der Satz angefügt:

VIII. Zwei algebraische Divisoren sind „absolut äquivalent", wenn jeder von beiden durch den anderen theilbar ist.

Ein algebraischer Divisor ist dann und nur dann äquivalent Eins, also überhaupt kein Divisor in der eigentlichen Bedeutung des Wortes, wenn die ganze algebraische Form, aus welcher derselbe gebildet worden, primitiv ist.

Das Beiwort „absolut" ist um desswillen hinzugefügt, weil später (S. 64) auch ein Begriff „relative Aequivalenz" eingeführt werden soll.

An die entwickelten Begriffsbestimmungen ist nun zunächst ein Satz zu knüpfen, welcher den Einheitscharakter der primitiven Formen darlegt und somit ein Fundamentaltheorem für die algebraischen Formen und Divisoren bildet.

IX. Wenn das Product von zwei ganzen algebraischen Formen, deren eine primitiv ist, für einen algebraischen Divisor congruent Null ist, so muss die andere Form selbst durch den Divisor theilbar sein.

Der aufgestellte Satz fällt unter die bereits in § 4 enthaltenen Entwickelungen, wenn in demselben ganze *rationale* Formen und Grössen an die Stelle der *algebraischen* gesetzt werden; denn alsdann sind Formen und Grössen nichts Anderes als ganze ganzzahlige Functionen von Variabeln und somit in irreductible Factoren zerlegbar. Auf diesen besonderen Fall kann aber der allgemeine Satz leicht zurückgeführt werden. Der Voraussetzung nach soll nämlich, wenn der Divisor der Hauptclasse angehört,

eine Gleichung

$$(A)\qquad F(u,v,w,\ldots).G(u,v,w,\ldots) = X.H(u,v,w,\ldots)$$

bestehen, in welcher X eine ganze algebraische Grösse und F, G, H ganze algebraische Formen bedeuten, von denen die erste primitiv ist. Mit u, v, w, ... sind die Unbestimmten der Formen bezeichnet. Aus der Gleichung (A) geht unmittelbar die folgende hervor:

$$(B)\qquad \mathrm{Nm}\left(z-\frac{G(u,v,w,\ldots)}{X}\right) = \mathrm{Nm}\left(z-\frac{H(u,v,w,\ldots)}{F(u,v,w,\ldots)}\right),$$

in welcher das Zeichen Nm, wie oben, das über alle conjugirten algebraischen Grössen und Formen erstreckte Product andeutet. Wird dieser Gleichung (B) die Gestalt gegeben

$$(C)\qquad \begin{aligned} &\mathrm{Nm}\,F(u,v,w,\ldots).\mathrm{Nm}\,(zX-G(u,v,w,\ldots)) \\ &= \mathrm{Nm}\,X.\mathrm{Nm}\,(zF(u,v,w,\ldots)-H(u,v,w,\ldots)), \end{aligned}$$

so sieht man, dass sie genau die oben erwähnten Voraussetzungen des zu beweisenden Satzes für den Fall rationaler Formen und Grössen enthält; denn an die Stelle der in der Gleichung (A) vorkommenden Formen und Grössen

$$F,\qquad G,\qquad X,\qquad H$$

sind in der Gleichung (C) die Ausdrücke

$$\mathrm{Nm}\,F,\quad \mathrm{Nm}\,(zX-G),\quad \mathrm{Nm}\,X,\quad \mathrm{Nm}\,(zF-H)$$

getreten, von denen der erste eine primitive ganze rationale Form mit den Unbestimmten u, v, w, ..., der zweite und vierte eine ganze rationale Form mit den Unbestimmten z, u, v, w, ... und der dritte eine ganze rationale Grösse des Bereichs darstellt. Mit Hülfe der Entwickelungen in § 4 ist daher aus der Gleichung (C) zu erschliessen, dass der zweite Factor auf der linken Seite durch den ersten Factor auf der rechten theilbar, also die linke Seite der Gleichung (B) *ganz* sein muss. Die Gleichung für z:

$$\mathrm{Nm}\left(z-\frac{G(u,v,w,\ldots)}{X}\right) = 0$$

ist somit eine solche, deren Coefficienten sämmtlich algebraisch ganz sind, und es ist also

$$\frac{G(u,v,w,\ldots)}{X}$$

algebraisch ganz, oder, der Behauptung des Satzes gemäss, $G(u,v,w,\ldots)$ durch X theilbar. — Wird nun endlich an Stelle der ganzen algebraischen

Grösse X ein Divisor, $\mathrm{mod}[\varphi x+\varphi' x'+\varphi'' x''+\cdots]$, genommen, in welchem $x, x', x'', \ldots$ ganze algebraische Grössen und $\varphi, \varphi', \varphi'', \ldots$ die verschiedenen Producte von Potenzen unbestimmter Grössen $\mathfrak{v}, \mathfrak{w}, \ldots$ bedeuten, so folgt aus der darnach modificirten Gleichung (A) die Relation

$$(A') \qquad FG\Phi = PH,$$

in welcher Φ und P durch die Gleichung

$$(\varphi x+\varphi' x'+\varphi'' x''+\cdots)\Phi = P.\mathrm{Fm}(\varphi x+\varphi' x'+\varphi'' x''+\cdots)$$

erklärt und zur Vereinfachung die Unbestimmten der verschiedenen Formen weggelassen sind. Die Gleichung (A') geht in (A) über, wenn G an Stelle von $G\Phi$ und X an Stelle von P gesetzt wird. Aus der obigen Entwickelung folgt daher, dass die Congruenz

$$G\Phi \equiv 0 \qquad (\mathrm{mod.}\, P)$$

bestehen muss, dass also, da

$$P = \Phi.\mathrm{mod}[\varphi x+\varphi' x'+\varphi'' x''+\cdots]$$

ist, G in der That, wie im obigen Satze behauptet worden, durch den mit $\mathrm{mod}[\varphi x+\varphi' x'+\varphi'' x''+\cdots]$ bezeichneten Divisor theilbar sein muss.

§ 16.

Die algebraischen Divisoren, welche aus Linearformen gebildet sind.

Jeder der allgemeineren Divisoren ist, wie nachher gezeigt werden wird, einem aus Linearformen gebildeten Divisor absolut äquivalent. Es genügt desshalb, die Eigenschaften dieser besonderen Divisoren darzulegen, welche in § 14 zuerst eingeführt worden sind, und es ist nothwendig, die Entwickelung damit zu beginnen, weil bei jenem Nachweise der Aequivalenz mit den allgemeineren Divisoren davon Gebrauch zu machen ist.

Die aus Linearformen entstandenen Divisoren haben, wie bereits in § 14 gezeigt worden ist, die Haupteigenschaft, dass *jede* Linearform durch einen Divisor theilbar ist, dessen Elemente die Coefficienten der Linearform bilden. Dies ist nach den in § 15 aufgestellten Definitionen in den Satz zu fassen:

I. Divisoren, welche dieselben Elemente haben, sind einander absolut äquivalent.

Hierbei sind, wie überhaupt zunächst, unter den Divisoren nur solche zu verstehen, die aus Linearformen hervorgehen. Mit der Begriffsbestimmung dieser besonderen Divisoren sind folgende Eigenschaften unmittelbar gegeben.

II. Jede Grösse, welche durch den algebraischen Divisor theilbar ist, kann dessen Elementen hinzugefügt werden, und es kann jedes Element weggelassen werden, welches für den aus den übrigen Elementen gebildeten Divisor congruent Null ist; d. h. bei den angegebenen Veränderungen wird der Divisor nur in einen absolut äquivalenten transformirt.

III. Der grösste gemeinsame Theiler von zwei algebraischen Divisoren wird durch einen dritten dargestellt, der die Elemente beider als Elemente enthält, so dass

$$\operatorname{mod}[x+u'x'+u''x''+\cdots+y+v'y'+v''y''+\cdots]$$

der grösste gemeinsame Theiler von

$$\operatorname{mod}[x+u'x'+u''x''+\cdots] \quad \text{und} \quad \operatorname{mod}[y+v'y'+v''y''+\cdots]$$

ist, wenn die Theilbarkeit eines Divisors in dem oben (§ 15, VII) definirten Sinne, d. h. als wirkliche Theilbarkeit seines Zählers aufgefasst wird.

Hieraus folgt jene Eigenschaft der algebraischen Divisoren, von welcher in § 14, S. 46 bei der Bildung derselben ausgegangen wurde, nämlich, dass jeder algebraische Divisor den grössten gemeinschaftlichen Theiler seiner Elemente darstellt. — Ist der grösste gemeinsame Theiler von zwei Divisoren äquivalent Eins, so haben sie „keinen gemeinsamen Theiler" in der eigentlichen Bedeutung des Wortes und können auch als „gegen einander relativ prim" bezeichnet werden.

IV. Das Product von zwei algebraischen Divisoren entsteht durch wirkliche Multiplication der Zähler, d. h. es ist

$$\operatorname{mod}[x+u'x'+u''x''+\cdots].\operatorname{mod}[y+v'y'+v''y''+\cdots]$$
$$\sim \operatorname{mod}[xy+w'xy'+w''x'y+\cdots],$$

da in der That erstens jedes einzelne Element des linearen Ausdrucks rechts

$$xy+w'xy'+w''x'y+\cdots,$$

also dieser Ausdruck selbst durch das Product links theilbar ist, und da zweitens jedes Glied des entwickelten Products

$$(x+u'x'+u''x''+\cdots)(y+v'y'+v''y''+\cdots)$$

ein Element des Moduls rechts bildet und also durch denselben theilbar ist.

V. Ist das Product von zwei algebraischen Divisoren durch einen dritten theilbar, und hat der erste Divisor mit dem dritten keinen gemeinsamen Theiler, so ist der zweite durch den dritten theilbar. Denn wenn die Elemente der drei Divisoren

$$x, x', x'', \ldots; \quad y, y', y'', \ldots; \quad z, z', z'', \ldots$$

sind, so ist für $\mathrm{mod}[z+w'z'+w''z''+\cdots]$ der Voraussetzung nach

$$(x+u'x'+u''x''+\cdots)(y+v'y'+v''y''+\cdots)\equiv 0,$$

also auch

$$(x+u'x'+u''x''+\cdots+z+w'z'+w''z''+\cdots)(y+v'y'+v''y''+\cdots)\equiv 0,$$

und der aus dem ersteren dieser beiden Factoren zu bildende Modul ist der Voraussetzung nach äquivalent Eins.

§ 17.

Die allgemeinen algebraischen Divisoren; ihre Aequivalenz mit den besonderen, welche aus Linearformen gebildet sind.

Abgesehen von der Definition der Hauptclasse (§ 15, V) ist bei den bisherigen Darlegungen über die „algebraischen Divisoren" vom Begriffe der Art oder Gattung kein Gebrauch gemacht worden. In der That bedarf es einzig und allein der Feststellung des Begriffs der mit einander „conjugirten" Ausdrücke $x+u'x'+u''x''+\cdots$, um die Norm und daraus den mit $\mathrm{Fm}(x+u'x'+u''x''+\cdots)$ bezeichneten Nenner des Divisors bilden zu können. Der Begriff der speciellen *Art* und damit auch der *Gattung* tritt aber von selbst auf, wenn man eine Anzahl ganzer algebraischer Grössen zusammen betrachtet, nämlich der Begriff derjenigen Art und Gattung niedrigster Ordnung, unter welcher dieselben enthalten sind, und in diesem Sinne ist mit dem Begriffe des grössten gemeinsamen Theilers von ganzen algebraischen Grössen $x, x', x'', \ldots$ auch der Begriff der Art gegeben, welche durch die Elemente $x, x', x'', \ldots$ bestimmt ist, sowie der Gattung, welcher die Art angehört.

Erst mit Festsetzung der Art oder eigentlich der Gattung, zu welcher die Art gehört, wird für einen algebraischen Divisor der Begriff der Irreductibilität bestimmbar, und dieser soll vorläufig in folgender Weise definirt werden, indem dabei — wie auch weiterhin — nur die *Haupt-Arten,* also diejenigen, welche *alle* ganzen Grössen einer Gattung umfassen, zu Grunde gelegt werden sollen.

I. Ein algebraischer Divisor ist „irreductibel“ oder „prim“ (Primmodul, Primtheiler, Primdivisor), wenn er durch keinen anderen „eigentlichen“ Divisor der festgesetzten Art oder Gattung theilbar ist, d. h. also, wenn er nur durch solche Divisoren der Art theilbar ist, die ihm selbst oder der Eins äquivalent sind.

Ich hebe ausdrücklich hervor, dass bei dieser Erklärung nur der Begriff der Theilbarkeit der Divisoren (nach § 15, VII), nicht der ihrer Zerlegbarkeit, d. h. ihrer Darstellbarkeit als Product von anderen Divisoren zur Anwendung kommt. Doch genügt diese beschränkte Definition zur Herleitung eines zweiten Fundamentalsatzes der Divisoren-Theorie, mit Hülfe dessen alsdann die Definition der Irreductibilität vervollständigt werden soll.

II. Algebraische Divisoren, welche dieselben Elemente haben, sind absolut äquivalent im Sinne der in § 15, VIII gegebenen Definition.

Um den Satz allgemein zu beweisen, genügt es offenbar, den Fall zu behandeln, wo einer der beiden Divisoren aus einer linearen Form hervorgegangen ist. Dass jeder andere algebraische Divisor durch einen solchen theilbar ist, folgt unmittelbar daraus, dass nach § 14 und § 16, I jedes einzelne Element eines Divisors, welcher aus einer Linearform gebildet ist, denselben als Theiler enthält. Es ist also nur noch andererseits der Nachweis zu führen, dass $x+u'x'+u''x''+\cdots$ durch $\mathrm{mod}[\varphi x+\varphi' x'+\varphi'' x''+\cdots]$ theilbar ist, wenn $x, x', x'', \ldots$, wie oben, ganze algebraische Grössen und $\varphi, \varphi', \varphi'', \ldots$ die verschiedenen Producte von Potenzen irgend welcher unbestimmten Grössen $v, w, \ldots$ bedeuten.

Gemäss der unter No. I gegebenen Definition der Irreductibilität und auf Grund des in § 16, V aufgestellten Satzes kann ein Product ganzer algebraischer Grössen einer bestimmten Gattung $\mathfrak{G}$ nur dann durch einen irreductibeln aus einer Linearform gebildeten Divisor theilbar sein, wenn einer der Factoren des Products durch denselben theilbar ist. Dieser Satz gilt ebenso für ganze algebraische *Formen* mit beliebig vielen Unbestimmten; denn wenn man denselben für den Fall von $m-1$ Unbestimmten als erwiesen voraussetzt und beide Factoren des Products nach steigenden Potenzen der m^{ten} Unbestimmten u entwickelt denkt, so ist aus der Annahme, dass in dem einen Factor nur die ersten h Coefficienten, in dem anderen nur die ersten k Coefficienten durch einen irreductibeln Divisor theilbar seien, unmittelbar zu erschliessen, dass in dem Product der beiden Factoren der Coefficient von u^{h+k} den irreductibeln Divisor nicht enthalten kann, da ja

dieser Coefficient — nur in Bezug auf die Theilbarkeit durch den Divisor betrachtet — sich auf das Product der beiden Coefficienten von u^h in dem einen, und von u^k in dem anderen Factor, die beide als nicht theilbar angenommen worden, reducirt. — Bedeutet nun $\mathfrak{G}$ irgend eine Gattung, unter welcher alle conjugirten algebraischen Formen $x+u'x'+u''x''+\cdots$ enthalten sind, und $\mathfrak{D}$ einen im Sinne dieser Gattung irreductibeln, aus einer Linearform gebildeten algebraischen Divisor von $\mathrm{Nm}(\varphi x+\varphi' x'+\varphi'' x''+\cdots)$, d. h. also einen Divisor desjenigen Theilers dieser Norm, welcher von den in $\varphi, \varphi', \varphi'', \ldots$ enthaltenen Unbestimmten $v, w, \ldots$ unabhängig ist, so muss nach jenem eben bewiesenen Satze einer der conjugirten des Ausdrucks $\varphi x+\varphi' x'+\varphi'' x''+\cdots$ durch $\mathfrak{D}$ theilbar sein, und es muss daher dieser Ausdruck $\varphi x+\varphi' x'+\varphi'' x''+\cdots$ selbst einen der conjugirten des Divisors $\mathfrak{D}$ als Theiler enthalten. Dividirt man demnach $\varphi x+\varphi' x'+\varphi'' x''+\cdots$ durch den bezüglichen Divisor, so erhält man als Quotienten wiederum eine ganze algebraische Form der Gattung $\mathfrak{G}$, und diese Divisionen sind so lange fortzusetzen, bis der Quotient eine primitive Form wird. Durch ein solches Verfahren erhält man also den Ausdruck $\varphi x+\varphi' x'+\varphi'' x''+\cdots$, von welchem ausgegangen wurde, als ein Product von irreductibeln, aus Linearformen hervorgegangenen algebraischen Divisoren und einer primitiven Form der Gattung $\mathfrak{G}$ dargestellt, und es wird daher, wenn man das Product der irreductibeln Divisoren nach der Multiplications-Regel (§ 16, IV) zu einem einzigen, aus einer Linearform gebildeten, algebraischen Divisor der Gattung $\mathfrak{G}$, $\mathrm{mod}[\mathfrak{u}\mathfrak{x}+\mathfrak{u}'\mathfrak{x}'+\mathfrak{u}''\mathfrak{x}''+\cdots]$, vereinigt:

$$(A)\qquad \varphi x+\varphi' x'+\varphi'' x''+\cdots = \mathrm{mod}[\mathfrak{u}\mathfrak{x}+\mathfrak{u}'\mathfrak{x}'+\mathfrak{u}''\mathfrak{x}''+\cdots]\,.\,\mathfrak{F}(\mathfrak{u}, \mathfrak{u}', \ldots v, w, \ldots),$$

wo $\mathfrak{F}$ eine primitive Form ist. Nur der *zweite* Factor rechts enthält die Unbestimmten $v, w, \ldots$ und ist daher eine lineare homogene Function der verschiedenen Producte von Potenzen derselben, welche mit $\varphi, \varphi', \varphi'', \ldots$ bezeichnet sind. Die Gleichung (A) repräsentirt daher lauter Gleichungen

$$(A')\qquad x^{(k)} = \mathrm{mod}[\mathfrak{u}\mathfrak{x}+\mathfrak{u}'\mathfrak{x}'+\mathfrak{u}''\mathfrak{x}''+\cdots]\,.\,\mathfrak{F}^{(k)}(\mathfrak{u}, \mathfrak{u}', \ldots) \qquad (k=0,1,2,\ldots),$$

in welchen $\mathfrak{F}^{(k)}$ ganze algebraische Formen der Gattung $\mathfrak{G}$ mit den Unbestimmten $\mathfrak{u}, \mathfrak{u}', \ldots$ sind, oder lauter Congruenzen

$$x^{(k)} \equiv 0 \quad (\mathrm{mod}[\mathfrak{u}\mathfrak{x}+\mathfrak{u}'\mathfrak{x}'+\mathfrak{u}''\mathfrak{x}''+\cdots]) \qquad (k=0,1,2,\ldots).$$

Sind $u', u'', \ldots$ neue Unbestimmte, so besteht also die Congruenz

$$x+u'x'+u''x''+\cdots \equiv 0 \quad (\mathrm{mod}[\mathfrak{u}\mathfrak{x}+\mathfrak{u}'\mathfrak{x}'+\mathfrak{u}''\mathfrak{x}''+\cdots]),$$

welche, verbunden mit der Gleichung (A) zeigt, dass

$$(x+u'x'+u''x''+\cdots).\mathfrak{F}(\mathrm{u},\mathrm{u}',\ldots v,w,\ldots)$$

durch $\varphi x+\varphi' x'+\varphi'' x''+\cdots$, also auch durch den mit $\mathrm{mod}\,[\varphi x+\varphi' x'+\varphi'' x''+\cdots]$ zu bezeichnenden allgemeineren algebraischen Divisor theilbar ist, und da $\mathfrak{F}$ eine *primitive* Form ist, so folgt aus jenem in § 15, IX aufgestellten ersten Fundamentaltheorem, dass in der That die Congruenz

$$x+u'x'+u''x''+\cdots\equiv 0 \quad (\mathrm{mod}\,[\varphi x+\varphi' x'+\varphi'' x''+\cdots])$$

und also die Aequivalenz

$$\mathrm{mod}\,[x+u'x'+u''x''+\cdots]\sim \mathrm{mod}\,[\varphi x+\varphi' x'+\varphi'' x''+\cdots]$$

besteht, welche den Inhalt des zu beweisenden zweiten Fundamentaltheorems bildet.

Da *jeder* algebraische Divisor, wie eben nachgewiesen worden, einem solchen äquivalent ist, der aus einer Linearform entsteht, so braucht man keine anderen als diese besonderen Divisoren anzuwenden. Der zweite Fundamentalsatz zeigt, dass, wenn man sich auf das Gebiet dieser besonderen Divisoren beschränken will, man auch bei der *Division* innerhalb desselben bleiben kann. Denn wenn ein Divisor $\mathrm{mod}\,[z+w'z'+w''z''+\cdots]$ durch einen anderen, $\mathrm{mod}\,[y+v'y'+v''y''+\cdots]$, theilbar sein soll, so muss nach der Definition (§ 15, VI) der Quotient, abgesehen vom Nenner des ersten Moduls, eine ganze algebraische Form sein, und der aus einer solchen gebildete Divisor ist eben stets einem Linearform-Divisor äquivalent. Um aber diesen entscheidenden Punkt noch genauer darzulegen, sei

$$\mathrm{Nm}(y+v'y'+v''y''+\cdots) = Q.\mathrm{Fm}(y+v'y'+v''y''+\cdots).$$

Wenn nun der Modul mit den Elementen z durch den Modul mit den Elementen y theilbar sein soll, so muss nach der Definition (§ 15, V und VI) der Ausdruck

$$(B) \qquad \frac{z+w'z'+w''z''+\cdots}{y+v'y'+v''y''+\cdots}\cdot\mathrm{Fm}(y+v'y'+v''y''+\cdots)$$

oder der damit übereinstimmende Ausdruck

$$(B') \qquad \frac{1}{Q}(z+w'z'+w''z''+\cdots)\cdot\frac{\mathrm{Nm}(y+v'y'+v''y''+\cdots)}{y+v'y'+v''y''+\cdots}$$

eine ganze algebraische Form sein. In dieser letzteren Gestalt (B') ist es evident, dass der Ausdruck *ganz* in Bezug auf die Unbestimmten v, w ist. Denkt man sich denselben nach den verschiedenen Producten von Potenzen der Unbestimmten v, w entwickelt und bezeichnet alle diese verschiedenen

Producte der Einfachheit halber mit $\varphi, \varphi', \varphi'', \ldots$, so nimmt der Ausdruck die Gestalt an

$$\varphi x + \varphi' x' + \varphi'' x'' + \cdots,$$

und die Coefficienten der von einander linear unabhängigen Functionen φ, φ', φ'', ..., welche mit $x, x', x'', \ldots$ bezeichnet sind, müssen nach der Voraussetzung *ganze* algebraische Grössen sein. Die Congruenz

$$(C) \qquad z + w'z' + w''z'' + \cdots \equiv 0 \quad (\mathrm{mod}\,[y + v'y' + v''y'' + \cdots]),$$

welche die Voraussetzung der Theilbarkeit des einen Divisors durch den anderen enthält, hat also eine Gleichung

$$(\bar{C}) \quad (\varphi x + \varphi' x' + \varphi'' x'' + \cdots) . \mathrm{mod}\,[y + v'y' + v''y'' + \cdots] = z + w'z' + w''z'' + \cdots$$

zur Folge, und aus dieser Gleichung soll nun die Aequivalenz (D)

$$\mathrm{mod}\,[x + u'x' + u''x'' + \cdots] . \mathrm{mod}\,[y + v'y' + v''y'' + \cdots] \sim \mathrm{mod}\,[z + w'z' + w''z'' + \cdots]$$

abgeleitet werden. Dass der Divisor auf der rechten Seite durch das Product der beiden Divisoren links theilbar ist, folgt aus der ersten Grundeigenschaft der Divisoren. Denn da jedes Element x durch $\mathrm{mod}\,[x + u'x' + u''x'' + \cdots]$ theilbar ist (vgl. § 16, I), so muss das Product auf der linken Seite der Gleichung $(\bar{C})$ und also auch $z + w'z' + w''z'' + \cdots$ durch das Product auf der linken Seite der Aequivalenz (D) theilbar sein. Damit aber auch andererseits das Product der beiden Divisoren auf der linken Seite der Aequivalenz (D) durch den Divisor auf der rechten theilbar sei, ist nothwendig und hinreichend, dass

$$(x + u'x' + u''x'' + \cdots)(y + v'y' + v''y'' + \cdots) . \mathrm{Fm}\,(z + w'z' + w''z'' + \cdots)$$

durch $z + w'z' + w''z'' + \cdots$, oder also, mit Rücksicht auf die Gleichung $(\bar{C})$, durch

$$(\varphi x + \varphi' x' + \varphi'' x'' + \cdots) . \mathrm{mod}\,[y + v'y' + v''y'' + \cdots]$$

theilbar sei. Es ist also nachzuweisen, dass der Ausdruck

$$\frac{x + u'x' + u''x'' + \cdots}{\varphi x + \varphi' x' + \varphi'' x'' + \cdots} \cdot \mathrm{Fm}\,(y + v'y' + v''y'' + \cdots) . \mathrm{Fm}\,(z + w'z' + w''z'' + \cdots)$$

ganz, d. h. eine ganze algebraische Form ist. Bezeichnet man diesen Ausdruck mit Φ und setzt

$$\frac{\mathrm{Nm}(z + w'z' + w''z'' + \cdots)}{\mathrm{Fm}(z + w'z' + w''z'' + \cdots)} = R,$$

so wird mit Hülfe der Gleichung $(\bar{C})$

$$\Phi R = G,$$

wo G die ganze algebraische Form

$$(x+u'x'+u''x''+\cdots)(y+v'y'+v''y''+\cdots)\cdot\frac{\mathrm{Nm}(z+w'z'+w''z''+\cdots)}{z+w'z'+w''z''+\cdots}$$

bedeutet. Da nun nach dem obigen zweiten Fundamentalsatz die Congruenz

$$x+u'x'+u''x''+\cdots \equiv 0 \quad (\mathrm{mod}[\varphi x+\varphi' x'+\varphi'' x''+\cdots])$$

besteht, also $\Phi.\mathrm{Fm}(\varphi x+\varphi' x'+\varphi'' x''+\cdots)$ oder

$$\frac{G}{R}\mathrm{Fm}(\varphi x+\varphi' x'+\varphi'' x''+\cdots)$$

eine ganze algebraische Form ist, so folgt aus dem ersten Fundamentalsatz (§ 15, IX), dass G selbst durch R theilbar sein muss, und dass daher Φ in der That eine ganze algebraische Form ist. Hiermit ist also der Nachweis geführt, dass aus der Congruenz (C) die Aequivalenz (D) hervorgeht, dass also, wenn ein algebraischer Divisor durch einen anderen theilbar ist, auch der Quotient wieder als ein eben solcher, aus einer Linearform gebildeter Divisor dargestellt werden kann.

Nunmehr kann auch an Stelle der obigen Irreductibilitäts-Definition (I) die folgende gesetzt werden:

I'. Ein algebraischer Divisor ist irreductibel oder prim, wenn er nicht einem Product algebraischer Divisoren der festgesetzten Gattung äquivalent ist.

Ferner kann als ein Corollar des obigen zweiten Fundamentaltheorems der Satz aufgestellt werden:

II'. Jedes Element eines beliebigen allgemeinen algebraischen Divisors ist durch denselben theilbar,

durch welchen jene erste Grundeigenschaft der in § 14 eingeführten besonderen Divisoren auf die allgemeineren ausgedehnt wird.

§ 18.

Die Zerlegung der algebraischen Divisoren in irreductible Factoren.

Zur vollen Begründung der in No. I des vorigen Paragraphen gegebenen Irreductibilitäts-Erklärung fehlt noch der Nachweis, dass es stets möglich ist, bei einem gegebenen algebraischen Divisor zu ermitteln, ob derselbe die Bedingungen der Irreductibilität erfüllt oder nicht. Es wird nun zwar später in § 25 noch gezeigt werden, wie die irreductibeln Divisoren

einer gegebenen algebraischen Grösse mit Hülfe weiterer Entwickelungen der Theorie direct aufzustellen sind, aber es erscheint doch angemessen, darzulegen, wie diese nothwendige Ergänzung der im vorigen Paragraphen enthaltenen Grundlagen der Theorie auch gleich Anfangs, wenn auch in einer weniger einfachen und eleganten Weise, erfolgen kann. Die Aufstellung der irreductibeln Divisoren braucht nur für die Haupt-Art, d. h. also für die Gattung zu erfolgen.

Um alle irreductibeln Divisoren einer gegebenen algebraischen Grösse aufzufinden, braucht man offenbar nur diejenigen zu suchen, die in ihrer Norm enthalten sind. Es genügt daher zu zeigen, wie die sämmtlichen irreductibeln Divisoren einer irreductibeln, ganzen rationalen Grösse des Bereichs $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$ zu bestimmen sind*). Für den Fall $\mathfrak{R} = 1$ ist dies eine Primzahl p, und man hat alsdann zuvörderst alle ganzen algebraischen Zahlen der Gattung aufzustellen, bei denen die Coefficienten der Elemente des Fundamentalsystems nicht negativ und kleiner als p sind. Hierauf denke man sich, wenn x alle jene algebraischen Zahlen repräsentirt, die sämmtlichen Divisoren $\operatorname{div}[x + up]$, und von denjenigen, die nicht äquivalent Eins sind, alle grössten gemeinsamen Theiler gebildet. Die Reihe dieser Divisoren enthält dann alle, durch welche p theilbar ist, und wenn man aus derselben diejenigen weglässt, welche äquivalent Eins sind, sowie diejenigen, welche andere Divisoren der Reihe als Theiler enthalten, so bleiben *alle verschiedenen algebraischen Primdivisoren von p* übrig. Denn sie genügen den hierfür aufgestellten Kriterien, nämlich durch keinen anderen Divisor — der ja ebenfalls ein Divisor von p sein müsste — theilbar und nicht äquivalent Eins zu sein. — Für den Fall von Variabeln $\mathfrak{R}$ erfolgt, im Anschluss an das so eben für $\mathfrak{R} = 1$ auseinandergesetzte Verfahren, die Bestimmung der irreductibeln Divisoren einer beliebigen irreductibeln, ganzen rationalen Grösse des Bereichs ganz analog, wie in § 6 die Bestimmung der Elemente eines Fundamentalsystems gegeben worden ist.

Dividirt man einen aus einer Linearform gebildeten algebraischen Divisor der Gattung $\mathfrak{G}$ durch einen der in ihm enthaltenen algebraischen Divisoren, so ist der Quotient gemäss den am Ende des vorigen Paragraphen

*) Es ist kaum nöthig zu bemerken, dass der Ausdruck „Irreductibilität" sich bei „irreductibeln, ganzen, *rationalen* Grössen des Bereichs $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$, wie schon in § 1 hervorgehoben worden, auf diesen Bereich selbst bezieht, dass also solche Grössen keine ganzen rationalen, wohl aber *algebraische* Divisoren haben können.

gegebenen Entwickelungen wieder ein solcher algebraischer Divisor; ***man gelangt daher durch fortgesetzte Division zur vollständigen Zerlegung eines algebraischen Divisors der Gattung 𝔊 in seine irreductibeln Divisoren, und diese ist auf Grund des Satzes*** § 16, V ***eine völlig bestimmte.*** Es ist also im Besonderen auch jede irreductible ganze rationale Grösse des Bereichs als ein Product irreductibler algebraischer Divisoren der Gattung 𝔊 darstellbar, und zwar kommt darin dann und nur dann wenigstens einer der Primdivisoren mehrfach vor, wenn jene ganze rationale Grösse ein Theiler der Discriminante der Gattung ist (vgl. § 25). Die ***verschiedenen*** irreductibeln algebraischen Divisoren einer und derselben irreductibeln ganzen rationalen Grösse des Bereichs sollen ***„verbundene algebraische Divisoren“*** oder ***„Factoren“*** (divisores conjuncti)*) genannt werden, während nach der bereits oben (S. 50) getroffenen Festsetzung zwei algebraische Divisoren ***„conjugirte“*** (divisores conjugati) heissen, wenn die Elemente des einen die (im gewöhnlichen Sinne) conjugirten des anderen sind. Das Product der verschiedenen, verbundenen Divisoren eines irreductibeln, ganzen rationalen Factors P der Discriminante der Gattung hat — da ein solcher Factor P, wie eben erwähnt, mindestens einen der verbundenen Divisoren mehrfach enthält — die Eigenschaft, dass es, zu einer gewissen Potenz erhoben, durch jene ganze rationale Grösse des Bereichs, welche mit P bezeichnet ist, theilbar wird. — Die Norm eines irreductibeln algebraischen Divisors ist der Potenz einer irreductibeln ganzen (rationalen) Grösse des Bereichs ($\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots$) äquivalent; der Exponent dieser Potenz soll die „Ordnung“ des irreductibeln Divisors bezeichnen. Für eine Gattung n^{ter} Ordnung ist daher die Summe der Ordnungen sämmtlicher verbundener irreductibler Divisoren einer irreductibeln ganzen rationalen Grösse gleich n, wenn diese nicht Theiler der Discriminante ist und also keinen der verbundenen algebraischen Divisoren mehrfach enthält.

*) Da der Ausdruck „conjugirt“ bereits seine bestimmte Bedeutung hat, musste für den neu auftretenden Begriff eine davon verschiedene Bezeichnung gewählt werden, und ich habe dafür in dem nächstverwandten und auch von *Gauss* bei den Grössen $a+bi$ angewendeten Ausdruck „numeri conjuncti“ eine geeignete Bezeichnung zu finden geglaubt. Dass bei *diesen* Grössen, wie auch bei den aus Wurzeln der Einheit gebildeten Zahlen, im Lateinischen der Ausdruck „numeri conjuncti“, im Deutschen und Französischen das Wort „conjugirt“ gebraucht wird, konnte keinen Gegengrund für jene Einführung bilden, weil in diesen Fällen — wie überhaupt in allen Fällen, wo die Gattung keine conjugirten hat und also eine *Galois*sche Gattung ist, — die beiden unterschiedenen Begriffe selbst sich decken.

Im Falle $\mathfrak{R} = 1$ lässt sich für jeden algebraischen Divisor der Gattung $\mathfrak{G}$ und der Art $\mathfrak{S}$ ein System solcher Zahlen aufstellen, die ein vollständiges Restsystem bilden. Die Anzahl der verschiedenen Zahlen dieses Systems ist der Norm des Divisors gleich oder äquivalent. Dies folgt, wenn es keine zu $\mathfrak{G}$ conjugirten Gattungen giebt, d. h. wenn $\mathfrak{G}$ eine *Galois*sche Gattung ist, unmittelbar daraus, dass erstens die Anzahl der Elemente eines Restsystems für ein Product von Divisoren stets gleich dem Producte der Zahlen ist, welche die Anzahl der Elemente für die einzelnen Divisoren bezeichnen, dass zweitens die Anzahl der Elemente für conjugirte Divisoren dieselbe ist, und dass drittens die Anzahl der Elemente eines Restsystems für einen Divisor m, wenn m eine gewöhnliche Zahl bedeutet, offenbar gleich m^n ist, da das Restsystem alsdann aus allen denjenigen Zahlen besteht, welche man erhält, wenn man den n Coefficienten der Elemente eines Fundamentalsystems alle modulo m incongruenten Werthe beilegt. Der allgemeine Satz über die Anzahl der Elemente eines Restsystems für eine *beliebige* Gattung lässt sich aus dem für eine *Galois*sche Gattung herleiten; er kann aber auch direct auf die besondere Art und Weise gegründet werden, wie sich für die Primdivisoren die Restsysteme aufstellen lassen. Mittels eben jenes Verfahrens, welches zur Aufstellung eines Fundamentalsystems einer Art und Gattung führt, lässt sich nämlich das Restsystem für einen Primdivisor h^{ter} Ordnung, dessen Norm p^h ist, so aufstellen, dass alle Zahlen nur lineare Functionen von h Elementen des Fundamentalsystems sind, und hieraus folgt dann, dass die Anzahl dieser in Bezug auf den Primdivisor incongruenten Zahlen genau p^h ist.

§ 19.

Die ganzen algebraischen Zahlen und ihre Divisoren. Das *Kummer*sche Princip der Aequivalenz.

Die in § 14 eingeführten, aus Linearformen gebildeten algebraischen Divisoren, deren Eigenschaften in den darauf folgenden Paragraphen entwickelt worden sind, genügen für den einfachsten Fall $\mathfrak{R} = 1$ vollkommen, um die Theorie der aus dem Rationalitäts-Bereich hervorgehenden algebraischen Grössen, d. h. also die Theorie der *algebraischen Zahlen* zu erledigen. Man braucht nur noch jene Aequivalenz-Bestimmung, welche Herr *Kummer* für seine idealen Divisoren aufgestellt hat, auf diese *wirklichen* algebraischen Divisoren zu übertragen, um auch die Theorie der einzelnen besonderen

„Arten" (Species) von algebraischen Zahlen zu vervollständigen. Da jedoch für die algebraischen Divisoren schon oben (§ 15, VIII) eine Aequivalenz-Bestimmung gegeben worden ist, so erscheint es nothwendig bei der Anwendung des

„Kummerschen Princips der Aequivalenz"

die neue *„weitere* Aequivalenz", welche durch die besondere „Art" der behandelten algebraischen Zahlen bedingt wird, mittels der Zusatzbestimmung „relativ" von jener *engeren* „absoluten" Aequivalenz zu unterscheiden.

Wenn zwei Divisoren φ und ψ die Eigenschaft haben, dass beide, mit einem und demselben Divisor χ multiplicirt, einem Divisor der Hauptclasse absolut äquivalent sind, so begründet dies eine speciell auf die „Art" bezügliche „relative Aequivalenz" der Divisoren φ und ψ. An die Stelle der angegebenen Bedingung für die relative Aequivalenz kann auch *die* gesetzt werden, dass zwei Divisoren der Hauptclasse, also zwei algebraische *Grössen* η, θ existiren, welche zur festgesetzten Art gehören und für welche die Divisorenproducte $\theta\varphi$ und $\eta\psi$ absolut äquivalent sind, so dass sich der Quotient relativ äquivalenter Divisoren $\frac{\varphi}{\psi}$ durch den Quotienten ganzer algebraischer Grössen $\frac{\eta}{\theta}$, multiplicirt mit einem Quotienten primitiver Formen, darstellen lässt. Relativ äquivalente Divisoren sind also solche, die sich im Sinne der absoluten Aequivalenz nur durch Factoren von einander unterscheiden, welche ganze algebraische Grössen der festgesetzten Art sind, und es sind also absolut äquivalente Divisoren a fortiori relativ äquivalent.

Die Gesammtheit der einander relativ äquivalenten Divisoren ganzer algebraischer Grössen einer Art constituirt eine *„Classe"*. Für den hier behandelten Fall der algebraischen Zahlen ($\mathfrak{R} = 1$) folgt nun unmittelbar nach der in § 6 meiner Doctordissertation angewendeten Methode (vgl. das Citat in § 14), dass die Anzahl der Classen endlich ist. Diese Methode beruht einzig und allein auf der Kenntniss der Anzahl der Elemente eines vollständigen Restsystems für einen complexen Modul, ob dieser nun — wie eben in meiner Dissertation — eine wirkliche gebrochene complexe Zahl, ob er ein Modulsymbol und zwar nach der *Kummer*schen Theorie eine „ideale Zahl" oder nach der *Dedekind*schen ein „Ideal" sei. Die allgemeine Anwendbarkeit jener Methode ist an sich einleuchtend; sie bildete den Ausgangspunkt meiner Untersuchungen über die allgemeineren complexen Zahlen, und ich hatte *Dirichlet* schon *vor* meiner Dissertation eine Arbeit

übergeben, in welcher nach jener Methode die Endlichkeit der Anzahl der Multiplicatoren für die Darstellung von Zahlen als Normen ganzer complexer Zahlen bewiesen war, allerdings nur für solche complexe Zahlen, die als ganze ganzzahlige Functionen einer ganzen algebraischen Zahl definirt sind.

Bedeutet N die der Norm irgend eines Divisors φ (absolut) äquivalente ganze Zahl, bestimmt man ferner eine ganze Zahl k gemäss der Bedingung

$$k^n \leqq N < (k+1)^n,$$

wo n, wie immer, die Ordnung der Gattung ist, und denkt man sich alle ganzen algebraischen Zahlen der Haupt-Art oder der Gattung gebildet, in denen die Coefficienten der n Elemente eines Fundamentalsystems nur die Werthe 0, 1, 2, ... k haben, so müssen mindestens zwei darunter sein, welche für den Modul φ einander congruent sind, da das gesammte Restsystem nur N, also weniger als $(k+1)^n$ Zahlen enthält. Es giebt daher ganze algebraische, durch den Divisor φ theilbare Zahlen der Haupt-Art, deren Coefficienten sämmtlich ihrem absoluten Werthe nach kleiner als k sind. Die Norm einer solchen Zahl ist kleiner als $M.N$, wenn M so beschaffen ist, dass die Normen aller algebraischen Zahlen, bei denen die Coefficienten der Elemente echte Brüche sind, die Zahl M nicht übersteigen. Hieraus folgt, dass die Anzahl der Divisoren-Classen endlich ist, und daraus wiederum, dass jeder Divisor zu einer gewissen Potenz erhoben, deren Exponent ein Theiler der Classenanzahl ist, ein Divisor der Hauptclasse wird. Diese Divisoren sind ganzen algebraischen Zahlen der Gattung 𝔊 absolut äquivalent; man kann also *jeden* Divisor durch eine Wurzel aus einer ganzen algebraischen Zahl der Gattung 𝔊 darstellen, und es genügt schon eine endliche Anzahl von solchen ganzen algebraischen Zahlen höherer Gattung, um jeden algebraischen Divisor der Gattung 𝔊 durch ein Product einer dieser Zahlen und einer *gebrochenen* algebraischen Zahl der Gattung 𝔊 auszudrücken. Sollen aber nur *ganze* algebraische Zahlen zur Darstellung der algebraischen Divisoren einer Gattung 𝔊 verwendet werden, so kann dies freilich auf unendlich vielfache Weise geschehen, doch lässt die bezügliche Frage eine nähere Präcisirung zu. Zuvörderst sei bemerkt, dass das Hinzunehmen ganzer algebraischer Zahlen anderer Gattungen zum Zwecke der Darstellung der Divisoren von 𝔊 nur in einer besonderen Weise, nämlich multiplicatorisch, zu erfolgen hat. Dieses Hinzunehmen ist also eine gewisse beschränkte Weise des „Adjungirens“ und möge demgemäss, im Anschluss

an *Eisenstein**), als ein *„Associiren“* bezeichnet werden. Da alle nur durch Einheiten von einander verschiedenen ganzen algebraischen Zahlen, als Divisoren, einander „absolut äquivalent“ sind, so kann jede associirte Zahl durch eine ihr absolut äquivalente ersetzt werden. Ferner sind bei Uebertragung der oben eingeführten Begriffsbestimmung zwei associirte Zahlen als relativ äquivalent zu bezeichnen, sobald sie sich nur durch Factoren von einander unterscheiden, welche Zahlen der Gattung 𝔊 sind. Wenn sich nun zunächst als zu associirende Zahlen gewisse Wurzeln aus ganzen algebraischen Zahlen der Gattung 𝔊 darbieten, so ist doch dabei zu beachten, dass diese — wenn *alle* Divisoren damit dargestellt werden sollen — nicht in einer Gattung zusammengefasst werden können. Es tritt daher die Frage auf, ob es dennoch eine bestimmte Gattung Γ giebt, welche zur Darstellung aller Divisoren genügt. Ist dies der Fall, so müssen sich alle jene Wurzeln aus unendlich vielen ganzen algebraischen Zahlen der Gattung 𝔊 durch Zahlen der Gattung Γ, multiplicirt mit Einheiten, darstellen lassen; diese Gattung Γ muss also, in *naturgemässer* Weise der Gattung 𝔊 associirt, den vollständigsten Aufschluss über alle Theilbarkeits-Fragen derselben geben. Aber nicht um das für die Behandlung der complexen Zahlen geeignetste *Mittel* zu erlangen**) — denn ich habe die in § 14 eingeführte Darstellung der Divisoren, welche einer anderen Art von Association ihre Entstehung verdankt, von Anfang an als ein durchaus naturgemässes, äusserst werthvolles Mittel angesehen — sondern weil es mir von vorn herein als ein erstrebenswerthes höchstes *Ziel* der Theorie der algebraischen Zahlen erschien, habe ich mich bemüht, die Frage der *zu associirenden Gattungen* zu ergründen. Auf die Wichtigkeit dieser Frage bin ich schon bei meiner ersten Beschäftigung mit den singulären Moduln der elliptischen Functionen aufmerksam geworden, und dieselbe fand sich alsdann bei der Erledigung der analogen Frage für algebraische Functionen einer Variabeln durch die *Weierstrass*sche transcendente Darstellung der Primfunctionen bestätigt. Die Auffindung aller derjenigen Resultate in der Theorie der allgemeinen complexen Zahlen, welche in der Theorie der aus quadratischen Gleichungen entstehenden Zahlen oder also

---

*) Vergl. *Crelles* Journal Bd. 28 S. 318. Der Association der Formen, im Sinne *Eisensteins*, entspricht, nach der hier eingeführten Terminologie, in der Theorie einer bestimmten Species algebraischer Zahlen genau die Association algebraischer Divisoren.

**) Vergl. Herrn *Dedekinds* Aufsatz „Sur la théorie des nombres entiers algébriques“ im Bulletin des Sciences mathématiques et astronomiques, 2me série, t. I, 1 p. 83. S. 50 der Separatausgabe.

in der Theorie der binären quadratischen Formen ihr vollkommenes Analogon haben, bot — sobald einmal die unzerlegbaren Divisoren in genügender Weise begrifflich fixirt und definirt waren — keinerlei Schwierigkeiten dar, da die von *Gauss* aufgestellten Principien mit Benutzung der *Dirichlet*schen Methoden dazu vollständig ausreichten, und ich habe schon im Jahre 1858 in einer Arbeit über die allgemeinen complexen Zahlen eben jene Resultate entwickelt*). Nur für die Frage der Association der Gattungen gab es in früheren Untersuchungen nichts Analoges; es war ein ganz neues, überraschendes und interessantes Phänomen, als mir bei der Beschäftigung mit der complexen Multiplication der elliptischen Functionen (im Winter 1856) Gattungen algebraischer Zahlen vor die Augen traten, welche in der angegebenen Weise mit den Gattungen von Quadratwurzeln negativer ganzer Zahlen associirt sind. Eine solche der Gattung $\sqrt{-n}$ associirte Gattung Γ liefert, wie ich schon in einer im Monatsbericht vom October 1857 abgedruckten Mittheilung hervorgehoben habe, die sämmtlichen, nach der *Kummer*schen Bezeichnung, idealen Divisoren der Gattung $\sqrt{-n}$; ihre Ordnung ist gleich der Classenanzahl für die Gattung $\sqrt{-n}$, und es haben überhaupt alle tieferen, auf die Composition und Classeneintheilung bezüglichen Eigenschaften der Gattung $\sqrt{-n}$ in den elementaren Eigenschaften der associirten Gattung Γ, so zu sagen, ihr Abbild. Durch dieses Beispiel belehrt, glaubte ich meine Arbeiten über die complexen Zahlen nicht eher veröffentlichen zu sollen, als bis ich denselben durch Erledigung jener Frage den eigentlichen Abschluss zu geben vermöchte, und ich habe eben darum auch die im *Kummer*schen Citat erwähnte Publication damals zurückgehalten. Aber ich habe mich nunmehr auf Grund anderweitiger Erwägungen (vergl. die Einleitung) um so eher dazu entschlossen, meine Methode der Behandlung der algebraischen Grössen und Zahlen hier zu entwickeln, als ich neuerdings, d. h. im Anfang des vorigen Jahres, zur aprioristischen Erkenntniss,

*) Auf die erwähnte Arbeit bezieht sich die Stelle in der *Kummer*schen Abhandlung über die allgemeinen Reciprocitätsgesetze: „*Ich kann in Betreff dieser, so wie überhaupt der allgemeinen Sätze, welche allen Theorieen complexer Zahlen gemein sind, auch auf eine Arbeit von Herrn Kronecker verweisen, welche nächstens erscheinen wird, in welcher die Theorie der allgemeinsten complexen Zahlen, in ihrer Verbindung mit der Theorie der zerlegbaren Formen aller Grade, vollständig und in grossartiger Einfachheit entwickelt ist*“. (Abhandlungen der Königl. Akademie der Wissenschaften zu Berlin 1859 S. 57). Ich hatte dieselbe Arbeit schon im Sommer 1858 *Dirichlet*, bei einer zu diesem Zwecke verabredeten Zusammenkunft in Ilsenburg, vorgelegt und deren Resultate näher erläutert.

nämlich zu einer von der analytischen Entstehung unabhängigen Auffassung der Natur jener den Gattungen $\sqrt{-n}$ associirten Gattungen gelangt bin und damit Gesichtspunkte für das Studium der allgemeinen Frage dieser Art der Association gewonnen habe.

Das *Kummer*sche Princip der Aequivalenz oder Classeneintheilung für die idealen Zahlen, welches im Anfange dieses Paragraphen erwähnt worden, ist für die Theorie der algebraischen Zahlen und in seiner weiteren Ausbildung auch für die allgemeine arithmetische Theorie der algebraischen Grössen von fundamentaler Bedeutung. Freilich lag es schon als Grundgedanke in der *Gauss*schen Theorie der Composition der quadratischen Formen verborgen; aber eben diesen Gedankenkern aus der formalen Umhüllung, mit welcher ihn *Gauss* umgeben hatte, herausgelöst und den etwas umständlichen Apparat mittels einer neuen Begriffsbestimmung entbehrlich gemacht zu haben, ist, was *Kummer*s Einführung der idealen Zahlen den grossen und dauernden Werth verleiht. Die *Kummer*sche, dem ursprünglichen abstracten Begriffe idealer Theiler adäquate *Ausdrucksweise* passt freilich nicht für jene wirklichen Divisoren, sei es, dass sie in der Form von Brüchen, sei es, dass sie als associirte ganze Zahlen, sei es, dass sie, wie in § 22, als associirte Formen erscheinen, aber die Idee des Idealen bleibt in der Anwendung des *Kummerschen Aequivalenz-Princips* für die — wie immer — definirten Divisoren erhalten. Dieses Princip der Aequivalenz oder der Classeneintheilung bildet den ganzen eigentlichen und neuen Inhalt der Theorie der idealen Zahlen. Als *Divisoren* hatte ich schon vorher in meiner Doctordissertation, sowie in allgemeineren oben erwähnten Untersuchungen, ideale Zahlen in der Form als wirkliche gebrochene Zahlen angewendet, und zwar, wie schon oben erwähnt, genau so, wie sie bei der *Kummer*schen Definition gebraucht werden*); aber die Idee, derartige

*) Vgl. die *Kummer*sche Abhandlung im 35. Bande des *Crelle*schen Journals S. 342. Die Theilbarkeit einer complexen Zahl $f(\alpha)$ durch einen Primfactor von q ist daselbst mit Hülfe einer complexen Zahl $\psi(\eta)$, deren Norm die Primzahl q nur in der ersten Potenz als Factor enthält, durch die Congruenz

$$f(\alpha)\,\Psi(\eta) \equiv 0 \pmod{q}, \quad \text{wo} \quad \Psi(\eta) = \frac{N\psi(\eta)}{\psi(\eta)} \quad \text{ist},$$

definirt. Als *Divisor* ist der so definirte ideale Primfactor von q nichts Anderes als der Bruch $\frac{q}{\Psi(\eta)}$, und dieser geht in den Bruch $\frac{p}{\varphi(\varepsilon)}$ über, welcher in § 6 meiner Doctordissertation als Modul eingeführt ist, wenn p an die Stelle von q gesetzt und die Periode mit ε, statt mit η, bezeichnet wird.

Divisoren nun auch selbständig zu betrachten und eine Begriffsbestimmung der Aequivalenz daran zu knüpfen, lag von der Auffassung der Divisoren als solcher weit ab. Ich meinerseits habe bei meinen Arbeiten über complexe Zahlen in den Jahren 1843 bis 1846 zu einer solchen Erkenntniss nicht durchzudringen vermocht. Als ich dann später in den Jahren 1856 und 1857 durch das Studium der complexen Multiplication der elliptischen Functionen veranlasst wurde, auf meine früheren Untersuchungen über complexe aus Wurzeln beliebiger ganzzahliger Gleichungen $F(x) = 0$ gebildete Zahlen zurückzukommen, konnte ich mich auf das bereits seit einem Jahrzehnt bekannte *Kummer*sche Princip stützen und bediente mich bei dessen Anwendung zuerst jenes in § 25 für allgemeine algebraische Grössen dargelegten Mittels der Zerlegung der *Congruenz* $F(x) \equiv 0$ für die verschiedenen Primzahlmoduln zur Erklärung der Theilbarkeit durch einen idealen Primfactor oder Divisor. Die Darstellung der Divisoren mit Hülfe von Linearformen benutzte ich nur zum Uebergang von den „idealen" Zahlen zu den zerlegbaren Formen. Die Schwierigkeit, welche die ausserwesentlichen Primfactoren der Discriminante — die ich wegen dieses unregelmässigen Verhaltens damals als „irregulär" bezeichnete — bei der Zerlegung der Congruenz $F(x) \equiv 0$ darboten, suchte ich Anfangs dadurch zu beseitigen, dass ich andere Gleichungen derselben Gattung zu Grunde legte. Bald aber nahm ich zu jenem „methodischen Hülfsmittel der unbestimmten Coefficienten" meine Zuflucht und legte, um jegliche Zufälligkeit der besonderen Wahl einer Gleichung auszuschliessen, eine „Fundamentalgleichung" (vgl. § 25), d. h. eine solche Gleichung zu Grunde, deren n Wurzeln lineare Functionen unbestimmter Grössen $u_1, u_2, \ldots u_n$ sind, und welche alle ganzzahligen Gleichungen der Gattung repräsentirt, sobald man sich für u_1, $u_2, \ldots u_n$ alle möglichen ganzen Zahlen gesetzt denkt.

So bildete die Aufstellung der „Fundamentalgleichungen" den ursprünglichen Zweck einer Untersuchung, welche in ihrem Verlauf den richtigen *Ausgangspunkt* der Theorie, die wahre allgemeine Form der complexen Zahlen zeigte und zugleich auf die Methode führte, durch Association von linearen Formen und Divisoren die *Ziele* der Theorie *„vollständig"* und *„auf die einfachste Weise"* zu erreichen (vgl. § 22).

Zur Begründung der Definition der relativen Aequivalenz gehört noch die Angabe eines Verfahrens, mittels dessen entschieden werden kann, ob zwei gegebene Divisoren äquivalent sind oder nicht. Die Frage der rela-

tiven Aequivalenz ist aber unmittelbar auf die Frage zurückzuführen, ob eine gegebene Zahl sich als Norm einer complexen Zahl darstellen lässt, und diese ist nach Ermittelung der Einheiten durch Discussion einer endlichen Anzahl von Normen complexer Zahlen zu erledigen.

§ 20.

Einführung von Divisoren-Systemen verschiedener Stufen.

Die in § 14 bis § 17 enthaltenen Entwickelungen zeigen, dass auch für Gattungs-Bereiche ($\mathfrak{R}'$, $\mathfrak{R}''$, $\mathfrak{R}'''$, ...), d. h. auch wenn zwischen den Grössen $\mathfrak{R}$ algebraische Beziehungen statthaben, der grösste gemeinschaftliche Theiler je zweier ganzen rationalen Grössen des Bereichs, also jeder nothwendige Divisor — ohne irgend welche Verallgemeinerung des Begriffes der Division und ohne irgend welche Uebertragung seiner eigentlichen Bedeutung — in Wirklichkeit dargestellt werden kann. Der Uebergang aus der Sphäre der ganzen *rationalen* Zahlen oder der ganzen *rationalen* Functionen von Variabeln in die Sphäre der ganzen *algebraischen* Grössen einer Gattung macht eben keine Erweiterung des Begriffes der Division erforderlich. Wohl aber zeigt sich eine solche Erweiterung als geboten, sobald man von den Bereichen, in denen keine Variable $\mathfrak{R}$ vorhanden ist, zu solchen mit Variabeln $\mathfrak{R}$, oder, falls von den Zahlen abgesehen wird, von Bereichen, wo nur eine Variable $\mathfrak{R}$ vorhanden ist, zu solchen mit zwei oder mehr Variabeln $\mathfrak{R}$ übergeht, während auch hier wieder der Schritt von den rationalen zu den algebraischen Grössen keinerlei neue Einführung nothwendig macht. *Diese Erhaltung der Begriffsbestimmungen beim Uebergang vom Rationalen zum Algebraischen* war die Forderung, welche mir von vorn herein als leitendes Princip bei der Behandlung der algebraischen Grössen gedient hat.

Ganze rationale Functionen mehrerer Variabeln können, wenn sie zu Systemen von zwei oder mehreren Functionen zusammengefasst werden, zwar auch noch einen allen gemeinsamen Theiler haben, aber sie können überdies *„Gemeinsames“* haben, welches sich, wenn sämmtliche Functionen gleich Null gesetzt werden, als ein Gebilde von gewisser Ausdehnung oder als eine Zusammenfassung, ein „Complex“ mehrerer algebraischer Gebilde verschiedener Ausdehnung charakterisiren lässt. Dieses „Gemeinsame“ kann mit Hülfe der allgemeinen Eliminations-Theorie auch als eine Eigenschaft der Functionen selbst definirt werden, d. h. ohne die Werthsysteme der

Variabeln, wofür die Functionen gleichzeitig verschwinden, und die sich daran knüpfende Anschauungsweise zu benutzen, ohne also denjenigen *„arithmetischen“* Boden zu verlassen, der für alle Rationalitäts-Bereiche $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$, wenn die Grössen $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots$ nicht als veränderliche sondern als unbestimmte und in ihrer Unbestimmtheit zu erhaltende Grössen aufgefasst werden, derselbe ist, wie für den der gewöhnlichen rationalen Zahlen. Das Studium des einer beliebigen Anzahl von ganzen Functionen mehrerer Variabeln „Gemeinsamen“ war es, wodurch ich im Jahre 1865 zu einer erneuten Behandlung der Eliminations-Theorie geführt worden bin, und es hat sich dabei jene „Interpolationsformel für ganze Functionen mehrerer Variabeln*)“ ergeben, welche die Bedeutung dessen, was als einer Anzahl von Functionen gemeinsam zu betrachten ist, in klares Licht treten liess. Die *Lagrange*sche Interpolationsformel war bis dahin nur in der, so zu sagen, trivialen Weise verallgemeinert worden, dass eine ganze Function von *mehreren* Variabeln $x_1, x_2, \ldots x_n$ aufgestellt wurde, welche vorgeschriebene Werthe annimmt, wenn der Variabeln x_1 einer der ν_1 Werthe beigelegt wird, für welche $F_1(x_1) = 0$ wird, der Variabeln x_2 einer der ν_2 Werthe, für welche $F_2(x_2) = 0$ wird, u. s. f. Aber bei dieser Weise der Verallgemeinerung zeigte sich weder irgend welche Schwierigkeit noch auch irgend welche Besonderheit; erst beim Wegfall der Beschränkung, die darin liegt, dass jede der Functionen F nur *eine* der Variabeln enthält, gewann die Frage an Interesse und die Lösung an Bedeutung. Soll nämlich eine ganze Function von $x_1, x_2, \ldots x_n$ gebildet werden, welche für die m durch die n Gleichungen

$$F_i(x_1, x_2, \ldots x_n) = 0 \qquad (i=1, 2, \ldots n)$$

definirten Werthsysteme

$$x_1 = \xi_{1k}, \quad x_2 = \xi_{2k}, \quad \ldots \quad x_n = \xi_{nk} \qquad (k=1, 2, \ldots m)$$

m vorgeschriebene Werthe annimmt, so bedarf man dazu — genau wie im Falle, wo $n = 1$ ist — nur der Lösung der Aufgabe unter der speciellen Voraussetzung, dass $m-1$ der vorgeschriebenen Werthe Null sind. Eine ganze Function von $x_1, x_2, \ldots x_n$, welche für die $m-1$ Werthsysteme

$$x_1 = \xi_{1k}, \quad x_2 = \xi_{2k}, \quad \ldots \quad x_n = \xi_{nk} \qquad (k=2, 3, \ldots m)$$

verschwindet, repräsentirt aber offenbar eine Verallgemeinerung des im Falle $n = 1$ aus der Division von $F_1(x_1)$ durch $x_1 - \xi_1$ hervorgehenden Resultats;

*) Vgl. meine Mittheilung im Monatsbericht der Akademie der Wissenschaften vom December 1865.

mit der Herstellung einer solchen Function war daher diejenige Erweiterung des Begriffes der Division gegeben, welche beim Uebergang von ganzen Functionen einer Variabeln zu Functionen mehrerer Variabeln erfordert wird. Denkt man sich die Functionen F_i als ganze homogene lineare Functionen von $x_1 - \xi_{1k}$, $x_2 - \xi_{2k}$, ... dargestellt, so dass

$$F_i = (x_1 - \xi_{1k}) F_{1i}^{(k)} + (x_2 - \xi_{2k}) F_{2i}^{(k)} + \cdots + (x_n - \xi_{nk}) F_{ni}^{(k)}$$

wird, so sind $F_{1i}^{(k)}$, $F_{2i}^{(k)}$, ... ganze Functionen von $x_1, x_2, \ldots x_n$ und ξ_{1k}, ξ_{2k}, ... ξ_{nk}. Die Determinante

$$|F_{hi}^{(1)}| \qquad (h, i = 1, 2, \ldots n)$$

ist dann eine ganze Function von $x_1, x_2, \ldots x_n$ und $\xi_{11}, \xi_{21}, \ldots \xi_{n1}$, welche für die $m-1$ Werthsysteme

$$x_1 = \xi_{1k}, \quad x_2 = \xi_{2k}, \quad \ldots \quad x_n = \xi_{nk} \qquad (k = 2, 3, \ldots m)$$

verschwindet und daher unmittelbar zur Herstellung einer allgemeinen Interpolationsformel verwendet werden kann. Eben diese Determinante hat nun offenbar die Eigenschaft, dass sie, mit einem der Ausdrücke $x_i - \xi_{i1}$ multiplicirt, eine homogene lineare Function von $F_1, F_2, \ldots F_n$ ergiebt; an Stelle der Theilbarkeit durch eine ganze Function $F(x)$ — im Falle einer Variabeln — tritt also für den Fall von mehreren Variabeln *die Darstellbarkeit als homogene lineare Function von mehreren ganzen Functionen* $F(x_1, x_2, \ldots x_n)$. Bei der Analogie mit der einfachen Division erscheint es wohl gerechtfertigt, zur Abkürzung der Ausdrucksweise, wie ich es in meinen Universitäts-Vorlesungen öfters gethan habe, das System der Elemente $F_1, F_2, \ldots F_n$ in Bezug auf die daraus gebildeten homogenen linearen Functionen als ein

Divisoren-System oder *Modulsystem* n^{ter} *Stufe* $(F_1, F_2, \ldots F_n)$

zu bezeichnen und der Congruenz

$$G(x_1, x_2, \ldots x_n) \equiv 0 \quad (\text{modd.}\, F_1, F_2, \ldots F_n)$$

die Bedeutung beizulegen, dass die ganze Function $G(x_1, x_2, \ldots x_n)$ sich als ganze homogene lineare Function von $F_1, F_2, \ldots F_n$ darstellen lässt, in welcher die Coefficienten ebenfalls ganze Functionen von $x_1, x_2, \ldots x_n$ sind. Jene Congruenz bezeichnet also das Bestehen einer Gleichung

$$G(x_1, x_2, \ldots x_n) = \sum_{h=1}^{h=n} P_h(x_1, x_2, \ldots x_n) F_h(x_1, x_2, \ldots x_n),$$

in welcher $P_1, P_2, \ldots P_n$ ganze Functionen der n Variabeln x bedeuten. Zwei Modulsysteme sind als „äquivalent" zu betrachten, wenn jede Function

des einen mit Beziehung auf das andere congruent Null ist. Die Aequivalenz

$$(F_1, F_2, \dots F_n) \sim (\Phi_1, \Phi_2, \dots \Phi_n)$$

ist demnach durch das System von Congruenzen

$$F_h \equiv 0 \ (\text{modd.}\, \Phi_1, \Phi_2, \dots \Phi_n), \quad \Phi_h \equiv 0 \ (\text{modd.}\, F_1, F_2, \dots F_n) \qquad {\scriptstyle (h=1,2,\dots n)}$$

definirt. Wird die Voraussetzung festgehalten, welche meinen Entwickelungen in der erwähnten Mittheilung vom Dec. 1865 zu Grunde liegt, nämlich dass die Discriminante des Gleichungssystems $F_1 = 0$, $F_2 = 0$, ... $F_n = 0$ von Null verschieden ist, so ist nicht bloss das System der Gleichungen

$$G(\xi_{1k}, \xi_{2k}, \dots \xi_{nk}) = 0 \qquad {\scriptstyle (k=1,2,\dots m)}$$

eine *Folge* der Congruenz

$$G(x_1, x_2, \dots x_n) \equiv 0 \quad (\text{modd.}\, F_1, F_2, \dots F_n),$$

sondern es geht auch umgekehrt diese Congruenz aus jenem System von Gleichungen hervor. Dies beruht darauf, dass sich die Resultante von $n+1$ ganzen Functionen von n Variabeln als ganze homogene lineare Function der $n+1$ Functionen darstellen lässt. Denkt man sich nämlich die $n+1$ Functionen $F_0, F_1, \dots F_n$ als *vollständige* ganze Functionen von $x_1, x_2, \dots x_n$, d. h. als vollständige Ausdrücke der Dimensionen $\nu_0, \nu_1, \dots \nu_n$ mit unbestimmten Coefficienten $c^{(0)}, c^{(1)}, \dots c^{(n)}$, so ist die Resultante eine ganze ganzzahlige Function aller dieser Coefficienten c, welche verschwindet, sobald die Coefficienten c irgend welche Werthe erhalten, wofür die $n+1$ Functionen F gleichzeitig Null werden können. Ersetzt man nun in der Resultante die Coefficienten $c^{(k)}_{000\dots}$, welche die von $x_1, x_2, \dots x_n$ unabhängigen Glieder der Functionen F_k bilden, durch die Differenzen $c^{(k)}_{000\dots} - F_k$, so werden die n Gleichungen $F = 0$ identisch erfüllt, und es ist daher auch die Resultante *identisch* gleich Null. Entwickelt man dieselbe nunmehr nach $F_1, F_2, \dots F_n$, so gelangt man zu dem oben bezeichneten Satze, dass sich die Resultante ganzer Functionen als homogene lineare Function derselben darstellen lässt, und zwar so, dass die Coefficienten ganze Functionen von $x_1, x_2, \dots x_n$ sind. Setzt man $F_0 = x - (u_1 x_1 + u_2 x_2 + \dots + u_n x_n)$, so wird die Resultante eine ganze Function von x. Wenn diese mit $F(x)$ bezeichnet wird, so ist also

$$F(u_1 x_1 + u_2 x_2 + \dots + u_n x_n) \equiv 0 \quad (\text{modd.}\, F_1, F_2, \dots F_n),$$

und die *Gleichung*

$$F(u_1 x_1 + u_2 x_2 + \dots + u_n x_n) = 0$$

stellt die Resolvente des Gleichungssystems

$$F_1 = 0, \quad F_2 = 0, \quad \dots \quad F_n = 0$$

dar. Wenn man die Resultante der allgemeinen $n+1$ Functionen $F_0, F_1, \dots F_n$, nachdem darin wie oben die Coefficienten $c^{(k)}_{000\dots}$ durch die Differenzen $c^{(k)}_{000\dots} - F_k$ ersetzt worden, nach einem beliebigen Coefficienten $c^{(i)}_{h_1, h_2, \dots h_n}$, welcher mit $x_1^{h_1} x_2^{h_2} \dots x_n^{h_n}$ multiplicirt ist, differentiirt, so erhält man eine identische Gleichung

$$-R' x_1^{h_1} x_2^{h_2} \dots x_n^{h_n} + \overline{R} = 0,$$

in welcher R' die partielle Ableitung der Resultante nach $c^{(i)}_{000\dots}$ und $\overline{R}$ die partielle Ableitung nach $c^{(i)}_{h_1, h_2, \dots h_n}$ bedeutet. Dabei sind aber immer noch in R' und $\overline{R}$ an Stelle der Coefficienten $c^{(k)}_{000\dots}$, und zwar für alle n Werthe $k = 1, 2, \dots n$, die Differenzen $c^{(k)}_{000\dots} - F_k$ zu denken. Lässt man nunmehr diese Differenzen wieder in die Coefficienten $c^{(k)}_{000\dots}$ selbst übergehen, so geht jene Gleichung offenbar in eine Congruenz für das Modulsystem $(F_0, F_1, \dots F_n)$ über, und für den obigen Fall $F_0 = x - (u_1 x_1 + u_2 x_2 + \dots + u_n x_n)$ resultirt daher eine Congruenz

$$P x_1^{h_1} x_2^{h_2} \dots x_n^{h_n} \equiv Q \quad (\text{modd.}\, F_1, F_2, \dots F_n),$$

in welcher P und Q ganze Functionen von $u_1 x_1 + u_2 x + \dots + u_n x_n$ bedeuten. Wenn endlich $P_1(x)$ so bestimmt wird, dass für jede Wurzel der Gleichung $F(x) = 0$

$$P(x) P_1(x) = 1$$

wird, so ist

$$P(x) P_1(x) \equiv 1 \quad (\text{modd.}\, F_1, F_2, \dots F_n),$$

also

$$x_1^{h_1} x_2^{h_2} \dots x_n^{h_n} \equiv P_1(x) Q(x) \quad (\text{modd.}\, F_1, F_2, \dots F_n),$$

und es geht hieraus hervor, ***dass jede ganze Function von*** $x_1, x_2, \dots x_n$ ***für das Modulsystem*** $(F_1, F_2, \dots F_n)$ ***einer ganzen Function der einen linearen Verbindung*** $u_1 x_1 + u_2 x_2 + \dots + u_n x_n$ ***congruent wird, und dass sich hierdurch jede Congruenz für dieses Modulsystem in eine solche für den einfachen Modul*** $F(x)$ ***verwandeln lässt.***

Die vorstehende Entwickelung, bei welcher ***allgemeine*** Functionen $F_1, F_2, \dots F_n$ zu Grunde gelegt worden, gilt auch noch für alle speciellen Functionen, sobald nur die Discriminante von Null verschieden ist; denn in diesem Falle ist R' nicht mit der Resultante zugleich Null und also $P(x)$

nicht congruent Null modd. $F_1, F_2, \dots F_n$. Unter der Voraussetzung, dass die oben mit $F(x) = 0$ bezeichnete Resolvente des Gleichungssystems

$$F_1 = 0, \quad F_2 = 0, \quad \dots \quad F_n = 0$$

nicht gleiche Factoren enthält, kann also die Zerlegung der ganzen Function einer Variabeln $F(x)$ unmittelbar auf die „Zerlegung des Divisoren-Systems $(F_1, F_2, \dots F_n)$" übertragen werden, wenn man die einzelnen den verschiedenen Factoren der Resolvente entsprechenden Gleichungssysteme bildet. Sobald eines dieser Gleichungssysteme mehr als n Gleichungen erfordert*), braucht man nur n lineare Verbindungen mit unbestimmten Coefficienten einzuführen, um zu erschliessen, dass die ganze Function von x, welche — gleich Null gesetzt — die Resolvente bildet, congruent Null für ein Modulsystem ist, dessen (mehr als n) Elemente — gleich Null gesetzt — jene Gleichungen bilden. Ist nämlich $F(x) = \Phi(x)\,\Psi(x)$, ist ferner

$\Phi(x) = 0$ die Resolvente des Gleichungssystems $\Phi_1 = 0,\ \Phi_2 = 0,\ \dots\ \Phi_r = 0$,
$\Psi(x) = 0$ die Resolvente des Gleichungssystems $\Psi_1 = 0,\ \Psi_2 = 0,\ \dots\ \Psi_r = 0$,

ist endlich $V(x, v_1, v_2, \dots) = 0$ die Resolvente von n Gleichungen

$$v_1\Phi_1 + v_2\Phi_2 + \cdots + v_r\Phi_r = 0, \quad v_1'\Phi_1 + v_2'\Phi_2 + \cdots + v_r'\Phi_r = 0, \quad \dots,$$

und ebenso $W(x, w_1, w_2, \dots) = 0$ die Resolvente von n Gleichungen

$$w_1\Psi_1 + w_2\Psi_2 + \cdots + w_r\Psi_r = 0, \quad w_1'\Psi_1 + w_2'\Psi_2 + \cdots + w_r'\Psi_r = 0, \quad \dots,$$

so ist $\Phi(x)$ der grösste von den unbestimmten Grössen v unabhängige Theiler von $V(x, v_1, v_2, \dots)$ und $\Psi(x)$ der grösste von den unbestimmten Grössen w unabhängige Theiler von $W(x, w_1, w_2, \dots)$. Ferner ist gemäss den obigen Darlegungen $V(x, v_1, v_2, \dots)$ congruent Null für das Modulsystem

$$(v_1\Phi_1 + v_2\Phi_2 + \cdots + v_r\Phi_r, \quad v_1'\Phi_1 + v_2'\Phi_2 + \cdots + v_r'\Phi_r, \quad \dots)$$

also auch

$$V(x, v_1, v_2, \dots) \equiv 0 \quad (\text{modd.}\ \Phi_1, \Phi_2, \dots \Phi_r);$$

endlich ist, wenn die verschiedenen Coefficienten der Glieder $v_1^{k_1} v_2^{k_2} \dots$ in $V(x, v_1, v_2, \dots)$ mit $\Phi(x)P_1(x)$, $\Phi(x)P_2(x)$, ... bezeichnet werden,

$$\Phi(x)P_1(x) \equiv 0, \quad \Phi(x)P_2(x) \equiv 0, \quad \dots \quad (\text{modd.}\ \Phi_1, \Phi_2, \dots \Phi_r)$$

und daher, weil der Voraussetzung nach nicht alle Functionen $P(x)$ einen und denselben gemeinsamen Theiler haben und desshalb Functionen $Q(x)$ existiren, für welche

*) Dass $n+1$ stets genügen, ist oben in § 10 nachgewiesen worden.

$$P_1(x)Q_1(x)+P_2(x)Q_2(x)+\cdots=1$$

wird,

$$\Phi(x)\equiv 0 \quad (\text{modd.}\, \Phi_1, \Phi_2, \ldots \Phi_r),$$

und ebenso

$$\Psi(x)\equiv 0 \quad (\text{modd.}\, \Psi_1, \Psi_2, \ldots \Psi_r).$$

Das Gleichungssystem

$$\Phi_i \Psi_k = 0 \qquad (i, k=1, 2, \ldots r),$$

welches aus r^2 Gleichungen besteht, wird offenbar nur erfüllt, wenn eines oder das andere der beiden Gleichungssysteme

$$\Phi_k = 0 \quad \text{oder} \quad \Psi_k = 0 \qquad (k=1, 2, \ldots r)$$

erfüllt wird, d. h. also, wenn die Resolvente $\Phi=0$ oder $\Psi=0$ befriedigt wird. Die Functionen Φ und Ψ haben aber der Voraussetzung nach keinen gemeinsamen Theiler, da $F(x)$ oder $\Phi(x)\Psi(x)$ keine gleichen Factoren enthält; es muss daher $\Phi\Psi=0$ oder $F=0$ die Resolvente des Gleichungssystems

$$\Phi_i \Psi_k = 0 \qquad (i, k=1, 2, \ldots r)$$

sein, ebenso wie diejenige des Gleichungssystems

$$F_k = 0 \qquad (k=1, 2, \ldots r),$$

und die beiden Modulsysteme

$$(\Phi_i \Psi_k) \quad \text{und} \quad (F_k) \qquad (i, k=1, 2, \ldots r)$$

sind demnach einander äquivalent. Hieraus geht als Regel für die Composition zweier Modulsysteme hervor, dass man die einzelnen Elemente des einen Systems mit je einem Elemente des anderen Systems zu multipliciren hat, um die sämmtlichen Elemente des componirten Systems zu erhalten.

Immer unter der Voraussetzung, dass die Discriminante von Null verschieden ist, muss der vorstehenden Darlegung gemäss das Modulsystem $(F_1, F_2, \ldots F_n)$ in ebensoviel „Factoren" zerlegbar sein wie die Function $F(x)$. Es gilt daher auch für Functionen mehrerer Variabeln der Satz, dass eine ganze Function $G(x_1, x_2, \ldots x_n)$, wenn sie für irgend ein Werthsystem zugleich mit den n ganzen Functionen $F_1, F_2, \ldots F_n$ verschwindet, nothwendig für das Modulsystem $(F_1, F_2, \ldots F_n)$ congruent Null sein muss, falls dieses irreductibel ist.

§ 21.

Die Eigenschaften der Divisoren-Systeme.

Die im vorigen Paragraphen aus der Eliminations-Theorie entwickelten Begriffsbestimmungen beruhen einzig und allein darauf, dass auch bei der Betrachtung homogener linearer Functionen *mehrerer* Elemente ganz ebenso von den Coefficienten abstrahirt wird, wie dies im Falle eines einzigen Elements durch die Construction des Congruenzbegriffes erfolgt und durch die *Gauss*sche Bezeichnungsweise zum Ausdruck gebracht ist. Wenn man nun diese Begriffsbestimmungen in die allgemeine Sphäre eines *beliebigen* Rationalitäts-Bereichs $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \dots)$ überträgt, so gelangt man zu folgenden Definitionen, welche der arithmetischen Behandlung der ganzen rationalen Functionen von $\mathfrak{R}'$, $\mathfrak{R}''$, $\mathfrak{R}'''$, ..., d. h. also der ganzen rationalen Grössen eines beliebigen Bereichs zu Grunde zu legen sind, um eine erschöpfende Darlegung alles dessen geben zu können, was einer beliebigen Anzahl solcher Grössen M_1, M_2, M_3, ... gemeinsam ist und also dem, im Falle $\mathfrak{R} = 1$, allein vorhandenen, grössten gemeinschaftlichen Theiler einer beliebigen Reihe ganzer Zahlen m_1, m_2, m_3, ... entspricht.

I. Jede homogene lineare ganze Function von M_1, M_2, M_3, ... mit ganzen, dem Bereich $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \dots)$ angehörigen Coefficienten wird als „das Modulsystem $(M_1, M_2, M_3, \dots)$ enthaltend“ oder auch als „congruent Null für dieses Modulsystem“ bezeichnet, und es ist

$$M \equiv M' \quad (\text{modd.}\, M_1, M_2, M_3, \dots),$$

wenn die Differenz $M - M'$ das Modulsystem $(M_1, M_2, M_3, \dots)$ enthält. Bei der vollkommenen Analogie mit dem einfachen Falle, wo die Anzahl der Elemente des Systems gleich Eins ist, erscheint es auch unbedenklich, wie schon oben, die Bezeichnung „Divisoren-System“ an Stelle von „Modulsystem“ zu gebrauchen, welche jener Analogie unmittelbareren Ausdruck giebt.

II. Ein Modulsystem $(M_1, M_2, \dots)$ enthält ein anderes $(M_1', M_2', \dots)$, wenn jedes Element des ersteren das Modulsystem $(M_1', M_2', \dots)$ enthält. Wenn jedes der beiden Modulsysteme das andere enthält, so sind sie einander äquivalent, und dies wird durch: $(M_1, M_2, \dots) \sim (M_1', M_2', \dots)$ bezeichnet.

III. Jede ein Modulsystem $(M_1, M_2, \dots)$ enthaltende Grösse kann dessen Elementen hinzugefügt werden, und es kann ebenso jedes Element eines Modulsystems weggelassen werden, welches für das durch die übrigen gebildete Modulsystem congruent Null ist; d. h. bei den angegebenen Veränderungen wird

das Modulsystem nur in ein äquivalentes transformirt. Wenn daher die Zahl Eins für ein Modulsystem $(M_1, M_2, \ldots)$ congruent Null ist, so ist dieses äquivalent Eins und also überhaupt kein Modulsystem im eigentlichen Sinne des Wortes.

IV. Das zwei Modulsystemen $(M_1, M_2, \ldots)$, $(M'_1, M'_2, \ldots)$ gemeinsame, d. h. in beiden zugleich enthaltene Modulsystem wird durch die Elemente beider gebildet, ist also durch das System $(M_1, M_2, \ldots, M'_1, M'_2, \ldots)$ repräsentirt, da offenbar *jedes* in den beiden ersten zugleich enthaltene Modulsystem auch in diesem dritten enthalten ist.

V. Ein Modulsystem $(M_1, M_2, \ldots)$, dessen einzelne Elemente durch die verschiedenen Producte von je zwei Elementen $M'_h M''_k$ zweier Modulsysteme $(M'_1, M'_2, \ldots)$, $(M''_1, M''_2, \ldots)$ gebildet werden, heisst „aus diesen beiden Systemen zusammengesetzt oder componirt", und diese beiden Systeme sollen, wegen der Analogie der Composition mit der Multiplication, auch als „Factoren" bezeichnet werden.

Der Ausdruck „Composition" soll ohne Weiteres auf äquivalente Systeme übertragen und demnach auch jedes dem System $(M'_h M''_k)$ äquivalente System als aus den beiden Systemen (M') und (M'') componirt bezeichnet werden, so dass die Elemente des componirten Systems als *bilineare* Functionen der beiderseitigen Elemente M', M'' mit ganzen dem Bereich angehörigen Coefficienten zu charakterisiren sind.

Ein Modulsystem $(M.M', M_1, M_2, \ldots)$ ist aus den beiden Systemen

$$(M, M_1, M_2, \ldots), \quad (M', M_1, M_2, \ldots)$$

zusammengesetzt, wenn das Modulsystem $(M, M') \sim 1$ ist, da dann stets je zwei bei der Composition entstehende Elemente $M_k M$, $M_k M'$ durch M_k zu ersetzen sind.

VI. Ein Modulsystem heisst irreductibel (oder ein Primmodulsystem), wenn es nicht aus zwei anderen zusammengesetzt ist, deren jedes ein Modulsystem im eigentlichen Sinne des Wortes ist.

VII. Enthalten die Grössen $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots$ nur genau $\mathfrak{n}-1$ von einander unabhängige variable oder unbestimmte Grössen $\mathfrak{R}', \mathfrak{R}'', \ldots \mathfrak{R}^{(\mathfrak{n}-1)}$, so giebt es Modulsysteme erster, zweiter, ... $\mathfrak{n}^{\text{ter}}$ *„Stufe"*, und daher auch Modulsysteme, die aus solchen verschiedener Stufe zusammengesetzt sind. Die Modulsysteme $\mathfrak{m}^{\text{ter}}$ Stufe sind an sich $\mathfrak{m}$-faltige Systeme und können nicht aus weniger als $\mathfrak{m}$ Elementen gebildet werden.

Bei der Zerlegung eines Modulsystems in seine den verschiedenen Stufen angehörigen Factoren ist genau so wie bei der Elimination zu ver-

fahren, nur dass auch noch die Zahlengrössen zu beachten sind. Es ist zuerst der grösste gemeinsame Divisor (im engeren Sinne des § 14), also der Divisor erster Stufe, aus allen Elementen herauszuheben; aus den vom grössten gemeinsamen Theiler befreiten Elementen sind nunmehr zwei lineare Functionen mit unbestimmten Coefficienten U zu bilden, und alsdann ist für eine der Variabeln $\mathfrak{R}'$, $\mathfrak{R}''$, ... z. B. für $\mathfrak{R}^{(n-1)}$ eine lineare Function aller mit unbestimmten Coefficienten u einzuführen. Wird diese mit $\mathfrak{R}$ bezeichnet, so enthält die nach Elimination von $\mathfrak{R}^{(n-2)}$ aus jenen beiden linearen Functionen entstehende Resultante nur noch die $\mathfrak{n}-2$ Variabeln $\mathfrak{R}$, $\mathfrak{R}'$, ... $\mathfrak{R}^{(n-3)}$. Von dieser Resultante ist der grösste von den Grössen U unabhängige Theiler, falls sie einen solchen hat, abzusondern, und es zerfällt alsdann das Modulsystem gemäss der unter No. V gegebenen Vorschrift — vorausgesetzt, dass die dort angegebene Bedingung erfüllt ist — in zwei Systeme, von denen das eine dem abgesonderten, das andere dem übrig gebliebenen Theiler der Resultante entspricht. Das erstere bildet das gesammte in dem ursprünglichen enthaltene Modulsystem zweiter Stufe, während das andere nur noch Modulsysteme höherer Stufen enthalten kann. Mit diesem ist alsdann ebenso zu verfahren. — Sind $\mathfrak{M}_1$, $\mathfrak{M}_2$, ... die Elemente eines Modulsystems $\mathfrak{m}^{\text{ter}}$ Stufe, und zwar eines solchen, welchem auch keine Systeme höherer Stufen beigemischt sind, so ist die Resultante von $\mathfrak{m}$ linearen Verbindungen mit unbestimmten Coefficienten U eine ganze Function von $\mathfrak{R}$, $\mathfrak{R}'$, ... $\mathfrak{R}^{(n-m-1)}$ und von den unbestimmten Grössen U, für den Fall $\mathfrak{m} = \mathfrak{n}$ also *nur* von diesen letzteren. Bezeichnet man nun den nach Absonderung des gesammten von den Grössen U unabhängigen Factors verbleibenden Theil der Resultante mit $\mathfrak{N}$, so bilden jene $\mathfrak{m}$ linearen Verbindungen der Elemente $\mathfrak{M}$, dividirt durch $\mathfrak{N}$, die $\mathfrak{m}$ Elemente eines Divisoren-Systems $\mathfrak{m}^{\text{ter}}$ Stufe, welches dem ursprünglichen aus beliebig vielen Elementen $\mathfrak{M}$ bestehenden System äquivalent ist. Dabei ist indessen vorausgesetzt, dass jener von der Resultante abgesonderte Factor aus lauter ungleichen Factoren besteht. Es ist ferner zu bemerken, dass die Resultante — falls noch algebraische Grössen $\mathfrak{R}$ vorhanden sind — immer mit Benutzung der bezüglichen Gleichung zu bilden ist.

Die angegebene Art, Modulsysteme $\mathfrak{m}^{\text{ter}}$ Stufe aus nur $\mathfrak{m}$ Elementen zu bilden, ist vollkommen analog jener Art, einfache Divisoren mit Hülfe linearer Functionen in Bruchform darzustellen. Sollen nur ganze rationale Grössen des Bereichs zu Elementen des Systems verwendet werden, so

genügt im Allgemeinen und zwar selbst bei natürlichen Rationalitäts-Bereichen nicht die der Stufenzahl gleiche Anzahl von Elementen, sondern es giebt auch Systeme, die mehr Elemente erfordern, ganz ähnlich wie es Gattungen algebraischer Grössen giebt, für welche die nothwendige Anzahl der Elemente des Fundamentalsystems die Ordnungszahl der Gattung übersteigt. Es erscheint daher angemessen, diejenigen irreductibeln Divisoren-Systeme, welche eine Darstellung durch eine der Stufenzahl gleiche Anzahl von Elementen gestatten, als zur „Hauptclasse" gehörig zu bezeichnen. Alsdann gehören offenbar, wenn unter den Grössen $\mathfrak{R}$ keine von den übrigen algebraisch abhängige vorkommen, alle irreductibeln Divisoren erster Stufe zur Hauptclasse. Wenn ferner die Anzahl der Grössen $\mathfrak{R}$ gleich Eins ist, wenn also die ganzen ganzzahligen Functionen *einer* unbestimmten Grösse $\mathfrak{R}'$ arithmetisch behandelt werden, so hat man noch Divisoren-Systeme zweiter Stufe zu betrachten, in denen eines der Elemente eine ganze Zahl, die übrigen aber ganze ganzzahlige Functionen von $\mathfrak{R}'$ sind. Diese Systeme sind also unmittelbar in solche zu zerlegen, bei denen die ganze Zahl die Potenz einer Primzahl p^m ist, und die übrigen Elemente sind hiernach nur im Sinne der Congruenz für den Modul p^m zu behandeln. Für $m = 1$ wird alsdann ein solches Divisoren-System zweiter Stufe nach der aus der Theorie der Congruenzen bekannten Weise als Product irreductibler Systeme von zwei Elementen $(F(\mathfrak{R}'), p)$ dargestellt, wo $F(\mathfrak{R}')$ eine ganze nach dem Modul p irreductible Function von $\mathfrak{R}'$ bedeutet. Diese Betrachtung zeigt die Theorie der höheren Congruenzen in einem neuen Lichte und bringt dieselbe mit ganz anderen zahlentheoretischen Gebieten in Verbindung. Es finden sich auch in dieser Theorie, sowohl in der von Herrn *Dedekind* aus *Gauss*' Nachlass publicirten Arbeit als in den *Schönemann*schen früher veröffentlichten Aufsätzen die ersten Andeutungen von Divisoren-Systemen zweiter Stufe, wenngleich nur unter beschränkterem Gesichtspunkte. Die naturgemässe und weitreichende Unterscheidung der Modulsysteme nach ihren verschiedenen Stufen, die Sonderung der in *Wahrheit* mehrfaltigen Divisoren-Systeme von denjenigen, die nur einfache Divisoren vertreten, konnte sich erst bei der arithmetischen Behandlung ganzer Functionen *mehrerer* Variabeln ergeben, und über diese ist bisher meines Wissens nichts bekannt gemacht worden. Wohl beruhen auch die *Dedekind*schen, nur den Fall $\mathfrak{R} = 1$ betreffenden Entwickelungen — nach der hier angenommenen Terminologie ausgedrückt — wesentlich auf der Betrachtung ganzer homogener linearer Functionen

mehrerer Elemente mit ganzen, dem Rationalitäts-Bereich angehörigen Coefficienten, also implicite auch auf der Betrachtung von „Divisoren-Systemen"; aber es sind dies — da bei algebraischen Zahlen überhaupt nur Divisoren erster Stufe vorhanden sind — doch nur solche, die die Stelle einfacher Divisoren vertreten. Ueberdies liegt grade darin, dass bei der *Dedekind*schen Auffassung die homogene lineare Function selbst, bei der meinigen aber das System der Elemente derselben als Divisoren-System den Ausgangspunkt bildet, noch eine gedankliche Verschiedenheit. In der That stellt Herr *Dedekind,* die Abweichung von der *Kummer*schen Auffassung selbst hervorhebend, den Inbegriff der durch einen idealen Divisor theilbaren wirklichen Zahlen an die Spitze der Entwickelung, während meine Begriffsbestimmungen von jeher, sowohl vor der Einführung der *Kummer*schen idealen Divisoren als nachher, in Uebereinstimmung mit der *Kummer*schen Gedankenrichtung auf die Erhaltung des Divisoren-Begriffes selbst zielten. Und dafür war gerade in den Elementen der homogenen linearen Functionen, wie sie bei der Behandlung von Functionen mehrerer Variabeln mit Nothwendigkeit an Stelle dessen auftraten, was der Divisor bei Functionen einer einzigen Variabeln ist, ein deutlicher Fingerzeig gegeben.

Divisoren-Systeme, welche die Stelle einfacher Divisoren vertreten, also nicht selbst Systeme höherer Stufe sind, können ebenso wie die gebrochenen Divisoren als Mittel der Untersuchung verwendet werden, aber die obige Zusammenfassung in Linearformen entspricht begrifflich und formal dem Zwecke am Besten. Die Beziehung der verschiedenen Darstellungsweisen der Divisoren lässt sich an den *Kummer*schen idealen Zahlen am Einfachsten erläutern. Sind nämlich nach den *Kummer*schen Bezeichnungen $\varphi(\alpha)$ und $\psi(\alpha)$ zwei äquivalente ideale Zahlen, die beide, mit derselben idealen Zahl $f(\alpha)$ multiplicirt, die wirklichen Zahlen $\Phi(\alpha)$ und $\Psi(\alpha)$ ergeben, und sind je zwei der drei idealen Zahlen ohne gemeinsamen Theiler, so kann offenbar der Bruch

$$\frac{\Phi(\alpha)}{\Psi(\alpha)} \quad \text{au Stelle des idealen Moduls} \quad \varphi(\alpha),$$

und das Divisoren-System

$$(\Phi(\alpha), \Psi(\alpha)) \quad \text{an Stelle des idealen Moduls} \quad f(\alpha)$$

verwendet werden. Dieses System von zwei Elementen ist aber nicht ein Modulsystem *zweiter Stufe,* da es nach der in § 14 dargelegten Weise, wenn

$$\text{Nm}\,(u\Phi(\alpha) + v\,\Psi(\alpha)) = \text{Nm}\,f(\alpha) \,.\, F(u, v)$$

ist, durch den einfachen Divisor

$$\frac{u\Phi(\alpha)+v\Psi(\alpha)}{F(u,v)}$$

ersetzt werden kann. Indessen lässt sich doch auch ein Ursprung jenes Divisoren-Systems von zwei Elementen in einem eigentlichen Modulsystem zweiter Stufe nachweisen. Bezeichnet man nämlich mit $X(x)=0$ die irreductible Gleichung, welcher α genügt, so kommen in der arithmetischen Theorie der ganzen ganzzahligen Functionen von x Divisoren-Systeme zweiter Stufe mit in Betracht, in denen $X(x)$ eines der Elemente ist. Alle diese besonderen Systeme sind, von einem anderen Gesichtspunkte aus betrachtet, Gegenstand der Theorie der complexen aus α gebildeten Zahlen, und die Zerlegung dieser Systeme in ihre irreductibeln Factoren stimmt mit der Zerlegung der complexen Zahlen in ihre idealen Primfactoren vollkommen überein (vgl. § 25). Das Verhältniss der einzelnen Theorieen complexer Zahlen zu der arithmetischen Theorie der ganzen ganzzahligen Functionen einer Variabeln, in der sie sämmtlich inbegriffen sind, lässt sich — wie überhaupt die besondere Natur der Modulsysteme höherer Stufen — am Deutlichsten darlegen, wenn die oben mit $\mathfrak{n}-1$ bezeichnete Anzahl der unabhängigen Variabeln $\mathfrak{R}$ grösser als Eins genommen wird. Nimmt man z. B. $\mathfrak{n}=4$ und denkt sich die drei Variabeln $\mathfrak{R}$ als irgend welche Coordinaten des Raumes, so sind die Divisoren erster Stufe entweder Zahlen oder ganze Functionen der Coordinaten, deren Verschwinden also Flächen repräsentirt. Unter den Divisoren-Systemen zweiter Stufe kommen hier solche vor, bei denen überhaupt nicht die sämmtlichen Elemente gleichzeitig verschwinden können und eines der Elemente als eine Zahl gewählt werden kann, aber auch solche, bei denen das gleichzeitige Verschwinden sämmtlicher Elemente eine Curve repräsentirt; unter den Modulsystemen dritter Stufe sind solche, die in ähnlicher Weise Punktsysteme darstellen. In die Hauptclasse jener Divisoren-Systeme zweiter Stufe gehören dann diejenigen Curven, welche den vollständigen Durchschnitt von zwei Flächen bilden, und man findet hierbei in überraschender Weise einen höheren Gesichtspunkt, von welchem aus die Frage der Darstellung ganzer Zahlen als Normen complexer Zahlen mit der Frage der isolirten Darstellung geometrischer Gebilde in der unmittelbarsten Beziehung erscheint. Endlich zeigt sich die Analogie jenes oben berührten Verhältnisses der arithmetischen Theorie der ganzen ganzzahligen Functionen einer Variabeln zu den einzelnen Theorieen complexer Zahlen für den Fall

$n = 4$ z. B. in dem Verhältnisse der analytischen Geometrie des Raumes zu den einzelnen „Geometrieen" auf besonderen algebraischen Flächen.

Die vorstehenden Entwickelungen enthalten nur die Einführung, keineswegs aber eine erschöpfende Behandlung der Modulsysteme höherer Stufen. So ist oben die Zerlegung solcher Modulsysteme nicht ganz allgemein sondern nur unter gewissen Einschränkungen erfolgt, deren Beseitigung vorbehalten bleiben muss. Die Erläuterung der hierbei auftretenden Fragen lässt sich schon an den einfachsten Fall der Divisoren-Systeme zweiter Stufe für den Fall einer einzigen Variabeln $\mathfrak{R}'$ anknüpfen, und es bietet sich dabei zugleich die Möglichkeit, die Besonderheiten der Divisoren-Systeme höherer Stufen im Vergleich mit den einfachen Divisoren principiell darzulegen. Setzt man die Variable x an Stelle von $\mathfrak{R}'$, so kommen in der Theorie der ganzen ganzzahligen Functionen von x die Divisoren-Systeme zweiter Stufe

$$(x, p), \quad (x^2, px, p^2), \quad (x^2+p, p^2), \quad (x, pq)$$

vor, wo p und q zwei verschiedene ungerade Primzahlen bedeuten sollen. Die drei letzten Modulsysteme enthalten offenbar das erste, und das zweite und vierte lässt sich auch als das Product je zweier Factoren darstellen, von denen der eine (x, p) ist; denn es ist in der That

$$(x^2, px, p^2) \sim (x, p)^2, \quad (x, pq) \sim (x, p)(x, q),$$

da $(x^2, px, qx, pq) \sim (x, pq)$ wird. Aber das dritte Modulsystem (x^2+p, p^2) ist, obgleich das erste im Sinne der oben gegebenen Definition „enthaltend", doch zugleich der bezüglichen oben entwickelten Begriffsbestimmung nach unzerlegbar; es enthält also das erste System nicht in der Weise, wie eine gewöhnliche Zahl einen ihrer Divisoren enthält, sondern etwa in der Weise, wie ein Gattungs-Bereich höherer Ordnung einen von niederer Ordnung enthält. Dieses von den Gesetzen der gewöhnlichen Theilbarkeit abweichende Verhalten bildet eine Besonderheit der Modulsysteme höherer Stufen. Behandelt man auch die Divisoren erster Stufe als Divisoren-*Systeme,* so muss nachgewiesen werden, dass sie eben diese Besonderheit *nicht* haben. Dies ist auch Herrn *Dedekind* nicht entgangen; in seiner höchst sorgfältigen und scharfsinnigen Art der Deduction, die bei seinen ganz abstracten Begriffsbestimmungen ebenso nothwendig als bewundernswerth erscheint, hat er in § 172 seiner „allgemeinen Zahlentheorie"*) den erwähnten Umstand ausdrücklich hervorgehoben.

*) Vorlesungen über Zahlentheorie, III. Auflage, Braunschweig 1879. Supplement XI. S. 521.

§ 22.

Die ganzen algebraischen Formen der verschiedenen Stufen; ihre absolute Aequivalenz; ihre Zerlegung in irreductible Factoren.

Für irgend einen Rationalitäts-Bereich oder eigentlich Integritäts-Bereich $[\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots]$, sei es ein natürlicher oder ein Gattungs-Bereich, ist nach der obigen Definition (§ 15, III) eine Form des Bereichs $[\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots]$ *primitiv,* wenn ihre Coefficienten keinen gemeinsamen Theiler haben. Aber nach den Ergebnissen der in §§ 20 und 21 gegebenen Entwickelungen bedeutet diese Bedingung nur, dass die Coefficienten keinen gemeinsamen Theiler *erster Stufe* haben sollen. Während also durch die in § 15, III aufgestellte Bedingung eine Form nur in Beziehung auf Divisoren erster Stufe primitiv wird, ist nunmehr mit Hülfe der Entwickelungen in den beiden vorhergehenden Paragraphen der Begriff des „Primitiven" enger zu fassen, und

> eine *eigentlich* primitive Form ist dadurch zu charakterisiren, dass ihre Coefficienten überhaupt keinen Divisor irgend einer Stufe mit einander gemein haben sollen.

Der Einfachheit halber sind hier bei dem Ausdruck „Form" die Beiwörter „ganz" und „algebraisch" weggelassen worden, und dies soll auch weiter in diesem Paragraphen geschehen, weil keinerlei Unklarheit dadurch entstehen kann. Ist F eine Form des Bereichs $[\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots]$ mit den Unbestimmten $u', u'', u''', \ldots$, und sind $U', U'', U''', \ldots$ die verschiedenen Producte von Potenzen der Unbestimmten $u', u'', u''', \ldots$ in der Entwickelung von F, so dass

$$F = M'U' + M''U'' + M'''U''' + \cdots$$

ist, wo die Coefficienten M „ganze" Grössen des Bereichs $[\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots]$ sind, so ist die Bedingung dafür, dass F eigentlich primitiv sei, die Aequivalenz

$$(M', M'', M''', \ldots) \sim 1,$$

nach den in § 21 gegebenen Begriffsbestimmungen. Eine Form ist also eigentlich primitiv, wenn das Modulsystem, dessen Elemente durch ihre Coefficienten gebildet werden, äquivalent Eins ist. Die hierbei hervortretende Beziehung der beiden Betrachtungsweisen, nämlich der einen, wonach die Grössen M ganz abstract als Elemente eines Systems betrachtet, und der anderen, wonach sie als Coefficienten einer Form zur Construction eines concreten Grössengebildes verwendet werden, soll nun zur Uebertragung der in § 21 enthaltenen Definitionen auf die Formen leiten, deren Coefficienten die Grössen M sind.

I. Eine Form soll als eine andere Form *„enthaltend“* bezeichnet werden, wenn das Coefficienten-System der letzteren in dem der ersteren (nach der in § 21, II gegebenen Bestimmung) enthalten ist.

II. Ist die Form F in der Form F_0, aber auch umgekehrt F_0 in F enthalten, so sind die beiden Formen einander „absolut äquivalent“ (vgl. § 21, II).

III. Jede eigentlich primitive Form ist absolut äquivalent Eins.

IV. Die Form $uF+F_0$, welche durch eine lineare Verbindung von irgend zwei Formen F und F_0 mit dem unbestimmten Coefficienten u entsteht, ist in jeder der beiden Formen F und F_0 enthalten, und bildet deren grössten gemeinsamen Inhalt (vgl. § 21, IV). Ist daher F in F_0 enthalten, so ist F der Form $uF+F_0$ absolut äquivalent.

V. Eine Form, welche durch wirkliche Multiplication von zwei anderen Formen entsteht, und jede einem solchen Product zweier Formen äquivalente Form soll auch, im Anschluss an die in § 21, V eingeführte Ausdrucksweise, die aus den beiden ersten zusammengesetzte oder componirte Form genannt werden.

VI. Eine Form wird als *„nicht zerlegbar“*, *„irreductibel“* oder als *„Primform“* bezeichnet, wenn sie keinem Producte von zwei *nicht primitiven* Formen des festgesetzten Bereichs $[\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots]$ äquivalent ist (vgl. § 21, VI).

VII. Enthalten die Grössen $\mathfrak{R}'$, $\mathfrak{R}''$, $\mathfrak{R}'''$, ... nur genau $\mathfrak{n}-1$ von einander unabhängige Variable $\mathfrak{R}'$, $\mathfrak{R}''$, ... $\mathfrak{R}^{(\mathfrak{n}-1)}$, so giebt es Formen erster, zweiter, ... $\mathfrak{n}^{\text{ter}}$ Stufe und auch Formen, die aus solchen verschiedener Stufen zusammengesetzt sind (vgl. § 21, VII).

Formen zweiter oder höherer Stufe und überhaupt solche, die keine Formen erster Stufe enthalten, sind zwar in dem früheren, weiteren Sinne primitiv, aber *uneigentlich* primitiv, und diese Eigenschaft des „uneigentlich Primitiven“ ist offenbar, wie die Formen selbst, verschieden „abgestuft“.

Formen $\mathfrak{m}^{\text{ter}}$ Stufe bestehen aus $\mathfrak{m}$ oder mehr Gliedern; diejenigen, welche nicht mehr als $\mathfrak{m}$ Glieder haben, deren Coefficienten-System also auch nur aus $\mathfrak{m}$ Elementen besteht, bilden nebst allen, die solchen Formen äquivalent sind, die Hauptclasse. In natürlichen Rationalitäts-Bereichen sind sämmtliche Formen erster Stufe

zur Hauptclasse gehörig, nicht aber alle Formen höherer Stufe (vgl. § 21).

VIII. Verschiedene Formen mit *denselben Coefficienten* sind einander absolut äquivalent, da die oben (unter I und II) gegebenen Definitionen überhaupt nur auf die Coefficienten der Form Bezug nehmen. Jede Form ist also einer *linearen* absolut äquivalent.

IX. Ist eine homogene lineare Form F in einer anderen F_0 enthalten, so lässt sich die erstere in die letztere dadurch transformiren, dass für die Unbestimmten von F Formen des Bereichs substituirt werden; diese Formen sind selbst linear, sobald auch F_0 eine lineare Form ist. In diesem Falle lässt sich also die enthaltene lineare Form F in die enthaltende Form F_0 durch eine lineare Substitution mit *ganzen* Coefficienten transformiren, und es ist dies zugleich eine *hinreichende* Bedingung für das Enthalten-Sein von F in F_0.

Die „lineare Substitution" bezieht sich natürlich auf die *Unbestimmten* der Formen, und unter „ganzen" Coefficienten sind solche zu verstehen, welche ganze rationale Functionen von $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots$, also *ganze* Grössen des Bereichs $[\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots]$ sind. Als Corollar des Satzes IX muss noch der Satz hervorgehoben werden:

X. Aequivalente homogene lineare Formen sind durch Substitutionen mit ganzen Coefficienten in einander transformirbar.

Wenn die Formen F, F_0 beziehungsweise die Elemente M, M_0 haben und also

$$(A) \qquad F_0 = \sum_h M_0^{(h)} u_0^{(h)}, \quad F = \sum_k M^{(k)} u^{(k)} \qquad (h=1, 2, \ldots; k=1, 2, \ldots)$$

ist, so bestehen gemäss der Definition I Relationen

$$(B) \qquad M_0^{(h)} = \sum_k C_{hk} M^{(k)} \qquad (h=1, 2, \ldots; k=1, 2, \ldots).$$

Es wird also

$$(C) \qquad F_0 = \sum_h \sum_k C_{hk} M^{(k)} u_0^{(h)} \qquad (h=1, 2, \ldots; k=1, 2, \ldots),$$

und die Form F wird demzufolge durch die Substitution

$$(\bar{C}) \qquad u^{(k)} = \sum_h C_{hk} u_0^{(h)} \qquad (h=1, 2, \ldots; k=1, 2, \ldots)$$

in die Form F_0 transformirt, wie es in dem mit IX bezeichneten Satze ausgesprochen ist.

Da nach § 14 oder § 17, II' jedes Element M durch den aus F gebildeten algebraischen Divisor theilbar ist, so hat, wie die Gleichung (C)

zeigt, auch die Form F_0 diese Eigenschaft, d. h. es ist

$$(D) \quad \mathrm{Fm}(M'u'+M''u''+M'''u'''+\cdots).F_0 \equiv 0 \quad (\mathrm{mod.}\,F).$$

Die Form F charakterisirt sich als reine Form erster Stufe dadurch, dass die mit $\mathrm{Fm}(M'u'+M''u''+M'''u'''+\cdots)$ bezeichnete Form eigentlich primitiv ist, da sonst die Norm von F ausser dem Divisor erster Stufe, welchen alle ihre Coefficienten mit einander gemein haben, noch Divisoren-Systeme höherer Stufen enthält. Wenn also eine solche Form F durch eine lineare Substitution mit ganzen Coefficienten in F_0 transformirt werden kann, so ist die Form F_0, multiplicirt mit einer eigentlich primitiven Form, durch F theilbar. Es lässt sich aber auch andererseits jene Transformirbarkeit aus dem, was sich hier als Consequenz ergeben hat, ableiten, wie jetzt gezeigt werden soll.

Es seien E, F, F_0 lineare oder nicht lineare Formen des Bereichs, und zwar E eine ***eigentlich*** primitive Form und F_0 eine ***reine Form erster Stufe;*** es sei ferner

$$F_0 = \sum_i M_0^{(i)} U_0^{(i)}, \quad F = \sum_k M^{(k)} U^{(k)},$$

wo $U_0^{(i)}$, $U^{(k)}$ Producte von Potenzen der Unbestimmten der Formen bedeuten. Nun soll angenommen werden, dass die Congruenz

$$(E) \quad E F_0 \equiv 0 \quad (\mathrm{mod.}\,F)$$

bestehe, so dass also auch F eine reine Form erster Stufe sein muss. Die angenommene Congruenz kann nach den in § 14 eingeführten Bezeichnungen auch in folgender Weise dargestellt werden:

$$(E') \quad E.\mathrm{Fm}(M_0' U_0' + M_0'' U_0''+\cdots).\mathrm{mod}\,[M_0' U_0' + M_0'' U_0''+\cdots] \equiv 0 \quad (\mathrm{mod.}\,F),$$

und hierbei ist $\mathrm{Fm}(M_0' U_0' + M_0'' U_0''+\cdots)$ eine ***eigentlich*** primitive Form, weil F_0 als reine Form erster Stufe vorausgesetzt worden ist. Auch das Product $E.\mathrm{Fm}(M_0' U_0' + M_0'' U_0''+\cdots)$ ist also eine eigentlich primitive Form, und diese möge, nach den Producten von Potenzen der Unbestimmten entwickelt, gleich $L'V'+L''V''+L'''V'''+\cdots$ sein. Alsdann geht die Congruenz (E') in

$$\mathrm{mod}\,[M_0' U_0' + M_0'' U_0''+\cdots].\sum_h L^{(h)} V^{(h)} \equiv 0 \quad (\mathrm{mod.}\,F)$$

über. Da auf Grund jenes zweiten Fundamentalsatzes (§ 17, II oder II') jedes Element der Form F_0 durch $\mathrm{mod}\,[M_0' U_0' + M_0'' U_0''+\cdots]$ theilbar ist, so ergiebt sich für jedes dieser Elemente $M_0^{(i)}$ die Congruenz

$$M_0^{(i)} \sum_h L^{(h)} V^{(h)} \equiv 0 \quad (\mathrm{mod.}\,F),$$

aus welcher die Congruenzen nach dem ***Modulsystem*** der Coefficienten von F

$$M_0^{(i)} L^{(h)} \equiv 0 \quad (\mathrm{modd.}\,M', M'', M''', \ldots)$$

und endlich, da das Modulsystem $(L', L'', L''', \ldots)$ äquivalent Eins ist, die Congruenzen

$$M_0' \equiv 0,\; M_0'' \equiv 0,\; M_0''' \equiv 0, \ldots \qquad (\text{modd.}\, M', M'', M''', \ldots)$$

hervorgehen. Diese Congruenzen enthalten die nothwendige und hinreichende Bedingung dafür, dass die Form F in F_0 enthalten und also F in F_0 durch eine Substitution mit ganzen Coefficienten transformirbar ist.

Aus der vorstehenden Entwickelung ergiebt sich, dass für reine Formen erster Stufe die obige Definition IX durch folgende ersetzt werden kann:

IX'. Eine Form F ist in F_0 enthalten, wenn eine eigentlich primitive Form E existirt, für welche das Product EF_0 wirklich durch F theilbar wird.

Für den Fall, dass diese Beziehung der beiden Formen eine gegenseitige ist, sind dieselben äquivalent, und man gelangt somit zu der neuen Aequivalenz-Bestimmung:

X'. Zwei Formen sind absolut äquivalent, wenn sie sich nur durch Factoren von einander unterscheiden, welche eigentlich primitive Formen sind.

Von den beiden verschiedenen Aequivalenz-Bestimmungen X und X' ist die erstere auf die Transformation, die letztere auf die Composition der Formen gegründet; die erstere stützt sich also auf das *Gauss*sche Princip der Aequivalenz, mit welchem die Theorie der quadratischen Formen in der V. Section der Disqq. Arithm. art. 157 beginnt, die letztere auf das *Kummer*sche Princip der Aequivalenz, welches in seiner Theorie der idealen Zahlen den Ausgangspunkt bildet, während es bei *Gauss* erst in der weiteren Entwickelung der Theorie (Disqq. Arithm. art. 234 sqq.) zur Anwendung kommt. Dass die beiden verschiedenen Definitionen, welche unter No. X und X' für die Aequivalenz der ganzen algebraischen Formen gegeben worden sind, sich vollkommen decken, bildet den Kernpunkt der obigen Auseinandersetzungen, und diese selbst basiren — wie wohl zu beachten ist — wesentlich auf jenem in § 17, II entwickelten zweiten Fundamentaltheorem.

Es ist offenbar der vollständige Einheitscharakter der *eigentlich* primitiven Formen, welcher durch jene zweite Definition der absoluten Aequivalenz X' zum natürlichen Fundament der arithmetischen Theorie der ganzen algebraischen Grössen und Formen gemacht wird, und auf diesem natürlichen Fundamente lässt sich auch die ganze Theorie am einfachsten aufbauen. So lassen sich z. B. die Hauptresultate, welche in den §§ 14 bis 18

an den Begriff der algebraischen Divisoren geknüpft worden sind, in der übersichtlichsten Weise als Hauptsätze der Formentheorie aussprechen, wenn man dabei die eigentlich primitiven Formen wirklich als Einheiten oder „Einheitsformen“ betrachtet und einfach

eine Form F als Factor oder Divisor einer Form F_0 bezeichnet, sobald diese Theilbarkeit von F_0 durch F im Sinne der absoluten Aequivalenz stattfindet, d. h. also, sobald F_0 multiplicirt mit einer eigentlich primitiven Form wirklich durch F theilbar wird.

Die beiden Fundamentalsätze (§ 15, IX und § 17, II) lauten alsdann folgendermassen:

XI. Absolut äquivalente Formen haben dieselben Theiler.

XII. Formen mit denselben Coefficienten sind äquivalent.

Die beiden Sätze legen also dar, dass erstens äquivalente Formen in Bezug auf die Division durch andere Formen einander ersetzen können, und dass zweitens die ganzen algebraischen Grössen, welche die Coefficienten der Formen bilden, das einzig Wesentliche derselben sind (vgl. No. VIII).

Endlich aber ist die in § 18 angegebene Zerlegbarkeit der Divisoren in den Satz zu fassen:

XIII. Jede ganze algebraische Form ist im Sinne der absoluten Aequivalenz als Product von irreductibeln Formen (Primformen) darstellbar und zwar nur auf eine einzige, also völlig bestimmte Weise.

Sowohl die Aequivalenz-Definition X′ als die hier daran geknüpften Darlegungen beziehen sich ausschliesslich auf reine Formen erster Stufe, d. h. also auf solche Formen

$$M'u' + M''u'' + M'''u''' + \cdots,$$

für welche die (schon in § 14) mit $\mathrm{Fm}(M'u' + M''u'' + M'''u''' + \cdots)$ bezeichnete Form *eigentlich* primitiv ist. Sie genügen aber vollständig für den einfachsten Fall der algebraischen Zahlen, wo keine Divisoren höherer Stufen existiren; sie genügen ferner, um die allgemeine Bedeutung zu würdigen, welche die Einführung der ganzen algebraischen Formen für die Theorie der algebraischen Grössen hat, und auch um die Art und Weise zu erkennen, in welcher die Resultate auf die Formen höherer Stufen auszudehnen sind.

Die „ganzen“ Grössen irgend eines natürlichen Rationalitäts-Bereichs mit den Elementen $\mathfrak{R}'$, $\mathfrak{R}''$, $\mathfrak{R}'''$, ..., d. h. also die ganzen ganzzahligen Functionen beliebig vieler unabhängiger Variabeln $\mathfrak{R}$ sind, wie in § 4 dargelegt ist, in irreductible Factoren zerlegbar, und zwar nur auf eine einzige,

also bestimmte Weise. Der Nachweis hierfür beruht einzig und allein darauf, dass

erstens ein Verfahren angegeben wird, mittels dessen die Zerlegung einer solchen Grösse in Factoren, die dem festgesetzten Grössenbereich angehören, bewirkt, also auch die Irreductibilität erkannt werden kann, und dass

zweitens der grösste gemeinsame Theiler zweier Grössen, also wenn sie gegen einander relativ prim sind, die Zahl Eins als lineare homogene Function derselben dargestellt werden kann und zwar mit Coefficienten, welche ebenfalls dem festgesetzten Grössenbereich entnommen sind.

Bezeichnet man dies als die beiden Erfordernisse der eindeutigen Zerlegung in irreductible Factoren, so ist bekanntlich das zweite nicht mehr allgemein erfüllt, sobald man von einem natürlichen Rationalitäts-Bereich zu Gattungs-Bereichen übergeht, und die dadurch bestimmten Grössenbereiche nicht weiter verändert. Erweitert man aber diesen Grössenbereich durch die Gesammtheit der ganzen algebraischen *Formen* des Gattungs-Bereichs, so wird dem zweiten Erforderniss entsprochen, und es wird in dieser erweiterten Sphäre algebraischer Gebilde immer noch sowohl jenem ersten als auch dem allgemeineren Erforderniss *der Erhaltung der algebraischen Rechnungsgesetze* vollkommen genügt, mit der einzigen Massgabe, dass durchweg an Stelle der Gleichheit die absolute Aequivalenz treten muss. So bildet z. B. die Gesammtheit der Formen mit beliebig vielen Unbestimmten, deren Coefficienten ganze algebraische *Zahlen* einer bestimmten Gattung sind, einen Bereich, in welchem alle Rechnungsoperationen sowie die einfachen Gesetze der gewöhnlichen ganzen Zahlen in vollem Umfange Geltung haben. Ebenso bleibt beim Uebergang von ganzen rationalen Functionen variabler $\mathfrak{R}$ zu ganzen algebraischen Functionen die eindeutige Zerlegbarkeit in irreductible Divisoren (erster Stufe) bestehen (vgl. XIII), wenn die Gesammtheit der Formen erster Stufe, unter welche die ganzen algebraischen Functionen selbst mit gehören, associirt wird. Wenn endlich zur vollständigen Entwickelung der Theorie der ganzen (rationalen und algebraischen) Functionen variabler Grössen $\mathfrak{R}$ auch die *Systeme* von Divisoren mit in Betracht gezogen werden, so ist die Association der Formen für die Erhaltung der Gesetze der Zerlegbarkeit erforderlich und ausreichend und zwar, was wohl zu beachten ist, ebenso bei natürlichen wie bei Gattungs-Bereichen, so dass

der Uebergang vom Rationalen zum Algebraischen auch hierin keinen Unterschied bedingt.

Bei der Definition der algebraischen Divisoren in §§ 14 und 15 und also auch bei deren Zerlegung ist von Divisoren höherer Stufen abstrahirt; die dort als primitiv bezeichneten Formen sind nicht *eigentlich* primitiv und können daher noch Divisoren höherer Stufen enthalten, und die Definition (§ 15, VIII) der Aequivalenz algebraischer Divisoren begründet also für die Formen, aus denen sie gebildet sind, nur eine „Aequivalenz *erster Stufe*". Bei jenen ersten Entwickelungen in Bezug auf die Divisoren sollte eben zur Erleichterung der Uebersicht nur der eine Schritt aus dem Gebiete der ganzen rationalen Functionen in das der algebraischen und nicht zugleich der andere Schritt von den Divisoren erster zu denen zweiter Stufe gemacht werden. Aber nachdem in den §§ 20 und 21 erst für natürliche und dann für beliebige Rationalitäts-Bereiche die Divisoren der verschiedenen Stufen eingeführt und behandelt worden sind, können auch die obigen Definitionen und Ergebnisse von den Formen erster Stufe auf die Formen höherer Stufe übertragen werden. An die Stelle der Definitionen IX′, X′ treten die allgemeineren für reine Formen $\mathfrak{m}^{\text{ter}}$ Stufe:

IX⁰. Bedeuten $F_1, F_2, \ldots F_{\mathfrak{m}}$ ganze algebraische Formen, welche sämmtlich dieselben Coefficienten haben und sich also nur durch die Systeme der Unbestimmten von einander unterscheiden, so ist eine dieser Formen in einer Form F_0 enthalten, wenn F_0 einer ganzen homogenen Function der $\mathfrak{m}$ Formen $F_1, F_2, \ldots F_{\mathfrak{m}}$ im Sinne der Definition X′ absolut äquivalent ist.

X⁰. Zwei Formen sind absolut äquivalent, wenn sie sich gegenseitig enthalten.

In der Definition IX⁰ ist die für die Formen erster Stufe gegebene Aequivalenz-Bestimmung X′ benutzt, implicite also auch in der Definition X⁰, welche auf jene erstere zurückgreift; aber jene Aequivalenz-Bestimmung X′ würde für Divisoren $\mathfrak{m}^{\text{ter}}$ Stufe zu eng und also nicht ausreichend sein. Die Aequivalenz-Bestimmung im Sinne der Definition X⁰ ist eine Folge derjenigen nach der Definition X′, aber nicht umgekehrt diese eine Folge jener.

Da bei jeder naturgemässen Aequivalenz-Bestimmung alle Formen mit denselben Coefficienten einander äquivalent sein müssen, so kann die Definition X⁰ auf zwei solche Formen angewendet werden. Alsdann muss eine Form $\mathfrak{m}^{\text{ter}}$ Stufe F, welche für andere und andere Systeme von Unbe-

stimmten, wie oben in IX^0 mit $F_1, F_2, \dots F_m$ bezeichnet werden möge, im Sinne der Aequivalenz-Bestimmung X$'$ als homogene lineare Function von $F_1, F_2, \dots F_m$ darstellbar sein. Dies kann zugleich als Definition für die Stufenzahl $\mathfrak{m}$ einer reinen Form F gelten, wenn nur noch hinzugefügt wird, dass keine kleinere Zahl als $\mathfrak{m}$ bei jener Darstellung ausreicht. Die allgemeine auf Formen aller Stufen bezügliche Aequivalenz-Bestimmung X^0 ist ebenso wie jene speciellere X$'$, welche für Formen erster Stufe gegeben worden ist, mit der früheren auf die Transformation gegründeten Definition der Aequivalenz in genauer Uebereinstimmung; sie gestattet auf Grund der Entwickelungen in den §§ 20 und 21 und nur, wie dort, mit Ausschliessung der Formen, die mehrfache Factoren enthalten, die Aufstellung des allgemeinen Satzes über die Zerlegung ganzer algebraischer Formen in ihre irreductibeln Factoren der verschiedenen Stufen, welcher als ein Hauptresultat hervorzuheben ist:

XIII^0. Jede ganze algebraische Form ist im Sinne der absoluten Aequivalenz X^0 als Product von irreductibeln Formen (Primformen) darstellbar, und zwar nur auf eine einzige, also völlig bestimmte Weise.

Dieser Satz zeigt, dass die Fundamentalgesetze der gewöhnlichen Zahlen auch in der allgemeinsten Sphäre algebraischer Grössen — bei Association der algebraischen Formen — noch Geltung behalten, und er legt zugleich jenes allgemeine Resultat der Eliminations-Theorie, welches in § 10 entwickelt worden ist, in dem umfassenderen Sinne der arithmetischen Theorie der algebraischen Grössen dar. Denn wenn $G', G'', G''', \dots$ ganze ganzzahlige Functionen von $\mathfrak{n}-1$ unabhängig veränderlichen Grössen $\mathfrak{R}'$, $\mathfrak{R}'', \mathfrak{R}''', \dots$ und $U', U'', U''', \dots$ die verschiedenen Producte von Potenzen unbestimmter Grössen $u', u'', u''', \dots$ bedeuten, so ist

$$(F) \qquad G'U' + G''U'' + G'''U''' + \cdots$$

nach § 15, I eine ganze rationale Form des Bereichs $[\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \dots]$, und durch die Gleichung

$$G'U' + G''U'' + G'''U''' + \cdots = 0,$$

welche das Gleichungssystem

$$(G) \qquad G' = 0, \quad G'' = 0, \quad G''' = 0, \quad \dots$$

repräsentirt, werden nach § 10 algebraische Beziehungen zwischen den Veränderlichen $\mathfrak{R}$ hergestellt, deren nähere Darlegung a. a. O. als die Aufgabe der Eliminations-Theorie bezeichnet ist. Wird nun die Form (F) nach XIII^0 als Product von Primformen dargestellt, so sind diese insofern von

zweierlei Charakter, als die einen für besondere Werthe der Variabeln $\mathfrak{R}$ gleich Null werden, die anderen aber nicht. Zu den letzteren gehören z. B. Primzahlen, welche etwa Divisoren von (F) sind. Die ersteren Primformen aber, welche nur von den ersten $n-1$ Stufen sein können, ergeben, gleich Null gesetzt, die verschiedenen irreductibeln Resolventen des Gleichungssystems (G), und die Systeme von Gleichungen, welche dadurch entstehen, dass die einzelnen Coefficienten je einer der Primformen gleich Null gesetzt werden, bilden die einzelnen, den verschiedenen Stufen angehörigen irreductibeln Theile jenes ursprünglichen Systems (G).

Die Association der ganzen algebraischen Formen, zu welcher die weitere Ausbildung jenes „methodischen Hülfsmittels der unbestimmten Coefficienten" geführt hat, bewirkt, wie das obige Hauptresultat XIII° zeigt, „die Erhaltung der Begriffsbestimmungen und Gesetze beim Uebergang vom Rationalen zum Algebraischen", welche im Anfange des § 20 als Forderung aufgestellt worden ist; sie gewährt den *„einfachsten"* erforderlichen und hinreichenden Apparat, um die arithmetischen Eigenschaften der allgemeinsten algebraischen Grössen *„vollständig"* und *„auf die einfachste Weise"* darzulegen. Die hervorgehobenen Ausdrücke sind dem ersten Satze von Herrn *Kirchhoffs* Mechanik entnommen, in welchem als die Aufgabe der Mechanik bezeichnet wird, die in der Natur vor sich gehenden Bewegungen *vollständig* und *auf die einfachste Weise* zu beschreiben. In dem Worte „beschreiben" wird hierbei mit Recht ein Hinweis auf den zu benutzenden wissenschaftlichen Apparat gegeben, und die *Kirchhoff*sche Forderung der Einfachheit ist ebensowohl auf die Mittel der Beschreibung als auf diese selbst zu beziehen. An sich könnte freilich die einfachste Darlegung mechanischer Vorgänge, auch wenn sie die ausgebildetsten Mittel der Analysis in Anspruch nimmt, genügend erscheinen, aber jener andere Vorzug der einfachsten Mittel, wie ihn *Dirichlets* Aufsatz über die Stabilität des Gleichgewichts*) zeigt, erfüllt, was die zweite *Kirchhoff*sche Forderung im höheren Sinne verlangt, dass die einfachsten Quellen der Erkenntniss aufzusuchen sind.

Die Association der Formen hat in der arithmetischen Theorie der algebraischen Grössen genau dieselbe Nothwendigkeit für sich wie die

---

*) Journal f. Mathematik Bd. 32, S. 85.

Association der imaginären zu den reellen Grössen in der Analysis und ist überhaupt in vielfacher Hinsicht damit vergleichbar. Ganz ähnlich wie die Linie der reellen Zahlen durch die „laterale Einheit"*) zur Ebene der complexen Zahlen sich ausdehnt, wird ein Grössenbereich $[\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots]$ durch die Unbestimmten der ganzen algebraischen Formen gewissermassen in Bezug auf seine „Dimension" erweitert, und *genau* ebenso wie der biquadratische Restcharakter in der Linie der reellen Zahlen nur von Punkten zu beiden Seiten derselben zu erkennen ist, sind die Gesetze der Erscheinungen an der Grenze des *Formen*gebietes, welche durch den ursprünglichen *Grössen*bereich gebildet wird, in der einfachsten Weise nur von Standpunkten aus darzulegen, welche im Innern des Gebietes der den Grössen associirten Formen liegen. So wie es ferner wohl angeht, die Eigenschaften der Functionen von $x+yi$ auch als solcher von x und y „vollständig" zu entwickeln, so können auch an Stelle der Formen erster Stufe die Systeme ihrer Coefficienten als Modulsysteme nach § 21 „vollständig" behandelt werden. In dem einen wie im anderen Falle würde jedoch bei solcher Behandlungsweise der zweiten *Kirchhoff*schen Forderung nicht genügt und das Wesentlichste der Einsicht und Erkenntniss entgangen sein.

Wenn einerseits die Zweckmässigkeit der Association der Formen durch die fast überraschende Einfachheit und Allgemeinheit der erzielten Resultate dargethan wird, so erscheint sie andererseits bei Bereichen mit variabeln Grössen $\mathfrak{R}$ auch vollkommen *angemessen,* weil die hinzugefügten algebraischen Gebilde ganz in der Sphäre der Betrachtung bleiben, und zwar so sehr, dass es vielmehr Sorgfalt erfordert, die Unbestimmten der Formen (u) von den Unbestimmten oder Variabeln $(\mathfrak{R})$, welche die Elemente des Bereichs bilden, nach ihren ganz verschiedenen Stellungen in der Entwickelung gehörig aus einander zu halten**). Aber für die aus dem absoluten Rationalitäts-Bereich $\mathfrak{R}=1$ hervorgehenden Gattungs-Bereiche, d. h. also für Bereiche algebraischer *Zahlen,* hat die Association der Formen mit ganzen algebraischen Coefficienten auf den ersten Blick etwas Fremdartiges; jedoch braucht man nur an die *Gauss*sche Einführung der quadratischen Formen in die reine Arithmetik zu erinnern, um den Schein des Fremdartigen aufzuheben. Vor *Gauss* kannte man nur quadratische Formen der *Zahlen;*

*) *Gauss* Werke Bd. II, S. 178.

**) In § 10 kommt eine ähnliche Unterscheidung zwischen den Variabeln z und $\mathfrak{R}$ vor.

erst *Gauss* hat bei den quadratischen Formen den früheren beschränkten Gesichtspunkt, bei welchem nur die Darstellbarkeit der Zahlen ins Auge gefasst wurde, fallen gelassen und Formen mit wirklichen „Unbestimmten" (indeterminatae) in die Arithmetik eingeführt. Diese ganz neue und von der früheren völlig abweichende Auffassung der quadratischen Formen ist eine der bewundernswerthesten Conceptionen seines weit- und scharfblickenden Geistes. Welche Wichtigkeit er selbst der Einführung der Unbestimmten in die Arithmetik beigelegt hat, zeigt sich an vielen Stellen seiner neuen, in ihren Haupttheilen darauf gegründeten, systematischen Behandlung der quadratischen Formen, und es sind namentlich die späteren Theile der Entwickelung, die Composition der Formen, die Darstellung der ternären durch binäre Formen, welche darauf beruhen. Die Nebenstellung, welche *Gauss* den Unbestimmten x, y in der Form $ax^2+2bxy+cy^2$ anweist, charakterisirt er gleich Anfangs durch die Bezeichnung (a, b, c), welche er für die Form einführt. Und in der That könnte die ganze *Gauss*sche Theorie der binären quadratischen Formen $ax^2+2bxy+cy^2$, nachdem die Aequivalenz durch die Transformationsgleichungen der Coefficienten erklärt ist, als eine Theorie der Systeme von drei Zahlen (a, b, c) aufgefasst und behandelt werden; aber wenn man so das Rechnungs-Substrat der Unbestimmten x und y ganz wegliesse, würde die Uebersicht der Operationen und Resultate bedeutend erschwert sein, und es würden auch wesentliche theoretische Gesichtspunkte damit verloren gehen. — Diese Darlegung kann auch zugleich als erläuterndes Beispiel für das oben erwähnte Verhältniss dienen, in welchem eine Theorie der abstracten Modulsysteme zur Theorie der mit dem Rechnungs-Substrat der Unbestimmten versehenen Formen steht.

Irgend eine Art der Association ist erforderlich; entweder der „analytische" oder der „dimensionale" Charakter der algebraischen Grössen muss erweitert werden, wenn beim Uebergange von der rationalen zur algebraischen Sphäre die Gesetze bezüglich der Zerlegung in Factoren vollständige Geltung behalten sollen. Während in der obigen Association der *Formen* eine dimensionale Erweiterung des ursprünglichen Grössenbereichs liegt, enthält jene Art der Association, welche in § 19 erwähnt worden ist, eine Modification des analytischen Charakters; denn die *Weierstrass*schen *transcendenten* Primfunctionen waren den *algebraischen* Functionen einer Variabeln, und die singulären Moduln der elliptischen Functionen waren den aus Quadratwurzeln gebildeten, also durch Kreistheilungsgrössen rational

darstellbaren, algebraischen Zahlen zu associiren. Auch die *Kummer*schen idealen Zahlen sind, wenigstens begrifflich, associirte Gebilde, und dass hierbei, wie bei der obigen Association der Formen, an Stelle der Gleichheit eine gewisse Aequivalenz tritt, findet sich ganz ebenso bei *jeder* stufenweisen Gebietserweiterung der Arithmetik*), welche durch das Hinzunehmen neuer Gebilde, also durch „Associiren" erfolgt.

§ 23.

Die relative Aequivalenz der ganzen algebraischen Formen.

Im vorigen Paragraphen ist ein ganz beliebiger Rationalitäts-Bereich zu Grunde gelegt und von jeder Unterscheidung der natürlichen und Gattungs-Bereiche abgesehen worden; es war dies nicht nur zulässig, sondern auch angemessen, um deutlich zu zeigen, dass die dort gegebenen Entwickelungen keinerlei Unterscheidung zwischen rationalen und algebraischen Functionen erheischen. Aber für die in diesem und in den folgenden Paragraphen enthaltenen Darlegungen ist eine solche Unterscheidung wesentlich, und es soll für dieselben desshalb ein natürlicher Rationalitäts-Bereich $[\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots]$ und eine bestimmte daraus hervorgegangene Gattung $\mathfrak{G}$ und Species $\mathfrak{S}$ algebraischer Grössen von vorn herein festgesetzt werden. Nunmehr lässt sich nach dem *Kummer*schen Princip der Aequivalenz (vgl. § 19) für die allgemeinsten ganzen algebraischen Formen in analoger Weise, wie es in § 19 für die algebraischen Zahlen und Divisoren erster Stufe geschehen ist, der Begriff relativer (durch die besondere Art $\mathfrak{S}$ bedingter) Aequivalenz aufstellen.

I. Zwei Formen irgend welcher Stufe sind relativ äquivalent, wenn beide, mit derselben Form zusammengesetzt (§ 22, V), einer ganzen algebraischen Grösse der Art $\mathfrak{S}$, also einer nach § 15, V der Hauptclasse zugehörigen Form absolut äquivalent sind.

Die hier aufgestellte Bedingung der relativen Aequivalenz ist stets hinreichend, aber nur für Formen erster Stufe zugleich nothwendig, und es wird unten (I'') für Formen höherer Stufen die allgemeinere gegeben werden. Aber um dahin zu leiten, muss diese erste beschränktere Bedingung noch etwas modificirt werden.

Zwei Formen F und F_0, welche die aufgestellte Bedingung erfüllen, müssen Gleichungen

$$F.\overline{F}.\Phi = X\Psi, \quad F'.\overline{F}.\Phi' = X'\Psi'$$

*) *Gauss* Werke Bd. II, S. 175.

genügen, in denen X, X' ganze algebraische Grössen und $\bar{F}$, Φ, Ψ, Φ', Ψ' ganze algebraische Formen der Species $\mathfrak{S}$ bedeuten, von denen die vier letzteren eigentlich primitiv sind. Hieraus folgt die Relation $FX'\Phi\Psi' = F'X\Phi'\Psi$, oder also, da $\Phi\Psi'$ und $\Phi'\Psi$ eigentlich primitive Formen der Species $\mathfrak{S}$ sind, die *absolute* Aequivalenz $FX' \sim F'X$, und zwar in dem engeren Sinne, ***welcher bei der Benutzung der absoluten Aequivalenz für die relative überhaupt durchweg festzuhalten ist****), dass die primitiven — als Factoren zur Verwandlung der Aequivalenz in eine Gleichung dienenden — Formen ebenfalls der für den Begriff der ***relativen*** Aequivalenz massgebenden Species angehören. Rechnet man nun zur ***Hauptclasse*** der Formen von $\mathfrak{S}$ alle diejenigen, welche den (schon nach § 15, V dazu gehörigen) ganzen algebraischen ***Grössen*** der Species $\mathfrak{S}$ in dem angegebenen engeren Sinne absolut äquivalent sind, so kann an Stelle der obigen Definition I eine Modification derselben gesetzt werden, welche der in § 22, X′ gegebenen Begriffsbestimmung der absoluten Aequivalenz vollkommen analog ist.

I′. Ganze algebraische Formen sind relativ äquivalent, wenn sie sich nur durch Factoren von einander unterscheiden, welche der Hauptclasse angehören. Im Sinne der relativen Aequivalenz verhalten sich also Formen der Hauptclasse wie Einheiten.

Diese Begriffsbestimmung der relativen Aequivalenz reicht auch für Formen höherer Stufe aus, wenn man darin die weiteren und allgemeineren, in § 22, VII und X⁰ gegebenen Bestimmungen der Hauptclasse und der absoluten Aequivalenz für die engeren (§ 15, V u. § 22, X′) substituirt.

Für die Formen ***erster*** Stufe ergeben sich ferner den in § 22, II und X aufgestellten Bedingungen der absoluten Aequivalenz entsprechende, nämlich:

II. Zwei ganze algebraische Formen erster Stufe F, F' sind relativ äquivalent, wenn die Coefficienten von F, multiplicirt mit einer ganzen algebraischen Grösse X' und die Coefficienten von F', multiplicirt mit einer ganzen algebraischen Grösse X, so beschaffen sind, dass sich die einen als homogene lineare Functionen der anderen und zwar so darstellen lassen, dass die Coefficienten der linearen Ausdrücke zum festgesetzten Art-Bereich ($\mathfrak{S}$) gehören.

*) Auch oben im § 19 (S. 64) ist die bei der relativen Aequivalenz benutzte absolute Aequivalenz der algebraischen Divisoren in dem engeren Sinne zu nehmen, dass der Zähler je eines algebraischen Divisors, dividirt durch den andern Divisor, gleich einer ganzen algebraischen Form ***der festgesetzten Art*** wird.

III. *Lineare* ganze algebraische Formen erster Stufe sind relativ äquivalent, wenn sie, multiplicirt mit je einer ganzen algebraischen Grösse der Art 𝔖, durch lineare Substitutionen mit ganzen, dem Art-Bereich (𝔖) angehörigen Coefficienten in einander transformirt werden können.

Die Aufstellung analoger Transformations-Bedingungen für die relative Aequivalenz von Formen höherer Stufen muss noch vorbehalten bleiben. Diese Bedingungen werden sich wohl einfacher aus derjenigen Auffassung ergeben, welche in § 25 dargelegt ist, wonach ganze *algebraische* Formen $\mathfrak{m}^{\text{ter}}$ Stufe eines Bereichs mit $\mathfrak{n}-1$ Variabeln $\mathfrak{R}$ durch ganze *rationale* Formen $(\mathfrak{m}+1)^{\text{ter}}$ Stufe eines Bereichs mit $\mathfrak{n}$ Variabeln $\mathfrak{R}$ zu ersetzen sind.

§ 24.

Die Fundamentalformen, insbesondere die linearen des algebraischen Zahlenreichs.

Um zu zeigen, dass die Darlegung der *allgemeinen* Eigenschaften der ganzen algebraischen Formen nur die einfachsten Mittel und namentlich keinerlei formalen Apparat erfordert, ist bisher von jeder „Reduction" der Formen abgesehen worden. Nunmehr soll aber eine solche Reduction auf gewisse „Grundformen" angegeben werden, um einige *speciellere* Entwickelungen daran knüpfen zu können.

Multiplicirt man die Elemente eines Modulsystems $(M', M'', M''', \ldots)$ der Gattung $\mathfrak{G}$ mit den sämmtlichen Elementen eines Fundamentalsystems von $(\mathfrak{G})$, so resultirt ein äquivalentes Modulsystem $(M_0', M_0'', M_0''', \ldots)$, welches die Eigenschaft hat, dass jede das Modulsystem M_0 enthaltende ganze Grösse des Gattungs-Bereichs $\mathfrak{G}$ sich als homogene lineare ganze Function von $M_0', M_0'', M_0''', \ldots$ mit ganzen dem Rationalitäts-Bereich $[\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots]$, also dem *Stammbereich* angehörigen Coefficienten darstellen lässt. *Alle* durch diese Eigenschaft charakterisirten Systeme M_0 — und es existiren solche auch in jeder besonderen *Species* 𝔖 — gestatten hiernach eine speciellere als die bisher angewendete Darstellungsweise, bei welcher Coefficienten der Gattung oder der Species selbst zugelassen wurden, und wenn diese auch, wie sich zeigen wird, von besonderem Interesse ist, so darf man sich doch nicht auf die Anwendung der specielleren Systeme M_0 beschränken, weil man sich dadurch mannigfacher Vortheile begeben würde. Die Systeme M_0 können nach der in §§ 6 und 7 angegebenen Weise auf äquivalente mit möglichst wenig

Elementen reducirt werden, und die Anzahl der Elemente dieser reducirten Systeme ist für $\mathfrak{R} = 1$ immer gleich n, d. h. gleich der Zahl, welche die Ordnung der Art $\mathfrak{S}$ bezeichnet. Irgend eine daraus gebildete Form, d. h. also eine Form, deren Coefficienten die Elemente jenes Modulsystems (M_0) sind, soll als *„Grundform“* oder *„Fundamentalform“* bezeichnet werden. Eine Form, deren Coefficienten die verschiedenen Elemente eines Fundamentalsystems der Species $\mathfrak{S}$ sind, ist demnach eine *„eigentlich primitive Fundamentalform“*.

Für den Fall des absoluten Rationalitäts-Bereichs $\mathfrak{R} = 1$, auf welchen jetzt näher eingegangen werden soll, existiren für alle Formen äquivalente lineare Grundformen von n Gliedern

$$u'x' + u''x'' + \cdots + u^{(n)}x^{(n)},$$

in welchen $x', x'', x''', \ldots$ ganze algebraische Zahlen des Art-Bereichs $(\mathfrak{S})$ bedeuten. Dies geht unmittelbar aus den vorstehenden allgemeineren Auseinandersetzungen hervor; doch soll die dem Gedanken nach höchst einfache Entwickelung, welche zu solchen Grundformen führt, zur besseren Uebersicht für den vorliegenden elementarsten Fall $\mathfrak{R} = 1$, hier noch ausführlich dargelegt werden.

Bedeuten $\mathfrak{x}', \mathfrak{x}'', \mathfrak{x}''', \ldots$ irgend welche ganze algebraische Zahlen eines Gattungs-Bereichs $(\mathfrak{G})$, von denen wenigstens eine, z. B. $\mathfrak{x}'$, zur Gattung $\mathfrak{G}$ selbst gehört und also von der Ordnung n ist, so bilden nach § 5 die ganzen ganzzahligen Functionen von $\mathfrak{x}', \mathfrak{x}'', \mathfrak{x}''', \ldots$ einen bestimmten mit $[\mathfrak{x}', \mathfrak{x}'', \mathfrak{x}''', \ldots]$ zu bezeichnenden Art-Bereich $(\mathfrak{S})$ des Gattungs-Bereichs $(\mathfrak{G})$; die *homogenen* ganzen Functionen von $\mathfrak{x}', \mathfrak{x}'', \mathfrak{x}''', \ldots$, d. h. diejenigen, welche bei der Darstellung als ganze Functionen kein von $\mathfrak{x}', \mathfrak{x}'', \mathfrak{x}''', \ldots$ unabhängiges Glied haben und also homogene ganze *lineare* Functionen der Grössen $\mathfrak{x}$ mit Coefficienten des Art-Bereichs $(\mathfrak{S})$ sind, füllen entweder den ganzen Bereich $(\mathfrak{S})$ aus, oder sie bilden einen Theilbereich $(\bar{\mathfrak{S}})$ von $(\mathfrak{S})$. Da schon die n^{te} Potenz jedes der Elemente $\mathfrak{x}$ sich als ganze ganzzahlige Function $(n-1)^{\text{ten}}$ Grades von $\mathfrak{x}$ darstellen lässt, so genügen alle diejenigen Producte von Potenzen der Elemente $\mathfrak{x}$, in welchen der Exponent kleiner als n ist, um jene homogenen Functionen sämmtlich als homogene ganze ganzzahlige lineare Functionen derselben auszudrücken. Bezeichnet man diese neuen, zur *linearen* Darstellung ausreichenden Elemente mit $\mathfrak{x}_0', \mathfrak{x}_0'', \mathfrak{x}_0''', \ldots$, so bildet

das System $(\mathfrak{x}_0', \mathfrak{x}_0'', \mathfrak{x}_0''', \ldots)$ ein Modulsystem von jener besonderen schon oben erwähnten Beschaffenheit, vermöge welcher sich jede das Modulsystem enthaltende Zahl der Art $\mathfrak{S}$ als homogene lineare Function der Elemente mit ganzzahligen, also dem Stammbereich $\Re = 1$ angehörigen Coefficienten darstellen lässt, und es ist auch für den Zweck dieser besonderen Darstellung offenbar jedem anderen $(\mathfrak{x}_1', \mathfrak{x}_1'', \mathfrak{x}_1''', \ldots)$ äquivalent, welches die Eigenschaft hat, dass jedes der Elemente des einen Systems eine homogene ganze ganzzahlige lineare Function des anderen ist. Denkt man sich nun in dem System $(\mathfrak{x}_0', \mathfrak{x}_0'', \mathfrak{x}_0''', \ldots)$ jedes der Elemente als homogene lineare Function von irgend welchen n derselben $\mathfrak{x}_0', \mathfrak{x}_0'', \ldots \mathfrak{x}_0^{(n)}$, die nur linear unabhängig sein müssen, dargestellt, so sind die Coefficienten rationale, ganze oder gebrochene Zahlen; und wenn man in allen diesen Ausdrücken die ganzzahligen Coefficienten durch Null ersetzt und die gebrochenen Coefficienten auf die durch ganzzahlige Differenzen von ihnen verschiedenen, positiven, echten Brüche reducirt, so resultirt ein äquivalentes System $(\mathfrak{x}_0', \mathfrak{x}_0'', \ldots \mathfrak{x}_0^{(n)}, \mathfrak{x}_1^{(n+1)}, \ldots)$, welches die ersten n Elemente mit dem ursprünglichen System gemein hat. Falls dieses System überhaupt noch aus mehr als n Elementen besteht, so muss der lineare Ausdruck von $\mathfrak{x}_1^{(n+1)}$ durch $\mathfrak{x}_0', \mathfrak{x}_0'', \ldots \mathfrak{x}_0^{(n)}$ wenigstens *eines* dieser n Elemente, z. B. $\mathfrak{x}_0'$, wirklich enthalten. Der Coefficient von $\mathfrak{x}_0'$ in dem linearen Ausdrucke ist dann ein echter Bruch, und es ist also die Discriminante der n ganzen algebraischen Zahlen $\mathfrak{x}_0'', \mathfrak{x}_0''', \ldots \mathfrak{x}_1^{(n+1)}$ kleiner als die Discriminante der ersten n Elemente $\mathfrak{x}_0', \mathfrak{x}_0'', \ldots \mathfrak{x}_0^{(n)}$. Da nun schon in dem System $(\mathfrak{x}_0', \mathfrak{x}_0'', \mathfrak{x}_0''', \ldots)$, von welchem ausgegangen wird, die ersten n Elemente als diejenigen angenommen werden können, deren Discriminante möglichst klein ist, so lässt sich das Resultat der obigen Deduction dahin formuliren,

> dass ein System von $n+1$ oder mehr ganzen algebraischen Zahlen $(\mathfrak{x}_0', \mathfrak{x}_0'', \mathfrak{x}_0''', \ldots)$ entweder durch ein solches ersetzt werden kann, welches nur n von den Elementen $\mathfrak{x}_0$ enthält, oder durch ein solches, in welchem eine der Discriminanten kleiner ist als die kleinste von allen, die aus den Elementen des ersteren Systems zu bilden sind.

Da indessen die Möglichkeit der Verkleinerung der Discriminanten einmal aufhören muss, so folgt schliesslich, dass *jedes* Modulsystem von ganzen algebraischen Zahlen n^{ter} Ordnung $(\mathfrak{x}_0', \mathfrak{x}_0'', \mathfrak{x}_0''', \ldots)$ durch ein Fundamentalsystem $(x', x'', \ldots x^{(n)})$ von nur n Elementen zu ersetzen ist. Für den Fall, dass die Zahl Eins das fundamentale Modulsystem $(x', x'', \ldots x^{(n)})$

enthält, ist dasselbe ein Fundamentalsystem der Art $\mathfrak{S}$ oder des Art-Bereichs ($\mathfrak{S}$).

Wird der Inhalt der vorstehenden Auseinandersetzungen gemäss § 22 von den „Modulsystemen" auf die „Formen" übertragen, so ergiebt sich, dass in dem hier behandelten Falle jede Grundform einer linearen mit nur n Coefficienten absolut äquivalent ist, und es kommt damit für die Theorie der ganzen algebraischen Formen, welche aus dem absoluten Rationalitäts-Bereich $\mathfrak{R} = 1$ hervorgehen, ein neues Element der Entwickelung hinzu. Um dies näher darzulegen, soll hier eine kurze übersichtliche Aufstellung dieser Theorie folgen, welche auch zeigen mag, dass die allgemeineren Resultate sich in der Anwendung auf diesen besonderen Fall vollständig bewähren.

Aus dem absoluten Rationalitäts-Bereich der rationalen Zahlen geht das Gesammtreich der ganzen algebraischen Formen hervor, deren Coefficienten irgend welche ganze algebraische Zahlen sind. Alle ganzen rationalen Functionen von Formen des bezeichneten Formenreichs, speciell auch alle ganzen algebraischen Zahlen, gehören selbst dazu, und man bleibt also bei jeder ganzen rationalen Operation innerhalb des bezeichneten Gebiets. Diesem gesammten Formenreiche selbst, nicht den einzelnen Gattungs- und Art-Bereichen von ganzen algebraischen Formen, welche dasselbe in sich schliesst, gehören die Begriffe des Conjugirt-Seins, der Norm*), des Enthalten-Seins und der absoluten Aequivalenz der Formen an, den einzelnen Art-Bereichen aber die Begriffe der relativen Aequivalenz und der Fundamentalform, und für den Begriff der Irreductibilität der Form ist der Gattungs-Bereich massgebend.

Eine ganze rationale Form ist primitiv, wenn ihre Coefficienten nicht sämmtlich einen gemeinsamen Theiler haben; eine ganze algebraische Form ist primitiv, wenn ihre Norm primitiv ist. In dem hier betrachteten Formenreiche sind alle primitiven Formen *eigentlich* primitiv. Die algebraischen Einheiten werden von der Gesammtheit der primitiven Formen mit umfasst, welche oben auch als Einheitsformen bezeichnet wurden. Eine Form F ist in einer anderen Form F_0 enthalten, wenn jeder Coefficient von F_0 sich als eine ganze lineare homogene Function der Coefficienten von F so darstellen lässt, dass die Coefficienten dieser Function ganze algebraische Zahlen

*) Nur der Begriff der „Partialnorm" gehört der einzelnen Gattung an.

werden (vgl. § 22, I und § 21, II). Die zweite hiermit sich völlig deckende Begriffsbestimmung für das Enthalten-Sein von F in F_0 ist hier fast wörtlich nach § 22, IX' anzufügen: Eine Form F ist in F_0 enthalten, wenn eine primitive Form (Einheitsform) E existirt, für welche das Product $E.F_0$ durch F, im gewöhnlichen Sinne des Wortes, theilbar wird. Zwei Formen sind absolut äquivalent, wenn sie sich gegenseitig enthalten. Jedes der Coefficienten-Systeme äquivalenter Formen ist also durch das andere in linearer homogener Weise mit ganzen algebraischen Coefficienten darstellbar, und der Quotient von zwei äquivalenten Formen ist gleich dem Quotienten von zwei primitiven. Dass Formen mit denselben Coefficienten, die sich also nur durch die Unbestimmten von einander unterscheiden, absolut äquivalent sind, folgt unmittelbar aus der ersteren der beiden Aequivalenz-Bedingungen. Jede primitive Form (Einheitsform) ist äquivalent Eins, also eine „Einheit" im Sinne der absoluten Aequivalenz. In demselben Sinne ist alsdann eine Form F, die in F_0 enthalten ist, als ein Theiler von F_0, und eine lineare homogene Function von zwei oder mehreren Formen $u'F' + u''F'' + \cdots$ mit den unbestimmten Coefficienten u', u'', ... als der grösste gemeinschaftliche Theiler von F', F'', ... zu bezeichnen.

Bei Festsetzung eines bestimmten Gattungs-Bereichs ($\mathfrak{G}$) ist jede ganze algebraische Form nach § 22, XIII einem unveränderlichen Product irreductibler Formen (Primformen) äquivalent. Bei Festsetzung eines bestimmten *Art-Bereichs* ($\mathfrak{S}$) der Ordnung n ist jede ganze algebraische Form einer linearen Grundform desselben Bereichs absolut äquivalent, also auch speciell einer solchen, die eine lineare Function von nur n Unbestimmten $u', u'', \ldots u^{(n)}$ mit ganzen algebraischen dem Art-Bereich ($\mathfrak{S}$) angehörigen Zahlcoefficienten ist, und es soll fernerhin in diesem Paragraphen der Ausdruck „Grundform" *nur* in der angegebenen engeren Bedeutung gebraucht werden. Primitive lineare Grundformen sind diejenigen, deren Coefficienten ein Fundamentalsystem des Art-Bereichs ($\mathfrak{S}$) bilden und zwar ein solches von nur n Elementen. Ist eine lineare Grundform F in irgend einer Form F_0 enthalten, so lässt sie sich nach § 22, IX in F_0 dadurch transformiren, dass für die Unbestimmten von F *ganzzahlige Formen* mit den Unbestimmten von F_0 substituirt werden, d. h. Formen, deren Coefficienten gewöhnliche ganze Zahlen sind. Wenn F_0 ebenfalls eine lineare Grundform ist, so sind auch die substituirten Formen linear, und es findet daher die Transformirbarkeit in dem gewöhnlichen Sinne des Wortes statt, dass die Form F in F_0 durch eine lineare ganz-

zahlige Substitution übergeführt werden kann. Für die absolute Aequivalenz linearer Grundformen ergiebt sich hieraus als nothwendige und hinreichende Bedingung, dass die eine in die andere durch eine ganzzahlige Substitution mit der Determinante Eins transformirt werden kann. Die Vergleichung mit der obigen auf die Composition gegründeten Aequivalenz-Bedingung führt daher zu dem Schluss, dass die Existenz einer Transformation von

$$\sum_h u^{(h)} x^{(h)} \quad \text{in} \quad \sum_k v^{(k)} y^{(k)} \qquad (h, k = 1, 2, \ldots n)$$

durch eine Substitution

$$u^{(h)} = \sum_k c_{hk} v^{(k)} \qquad (h, k = 1, 2, \ldots n)$$

oder

$$y^{(k)} = \sum_h c_{hk} x^{(h)} \qquad (h, k = 1, 2, \ldots n)$$

mit ganzzahligen Coefficienten c, deren Determinante gleich Eins ist, zugleich die Existenz von zwei primitiven Formen E, E' mit den Unbestimmten u, v bedingt, für welche die Gleichung

$$(u'x' + u''x'' + \cdots + u^{(n)}x^{(n)}).E = (v'y' + v''y'' + \cdots + v^{(n)}y^{(n)}).E'$$

besteht. Eine solche Gleichung begründet nach § 15 die Aequivalenz der beiden aus den Linearformen gebildeten Divisoren

$$\text{mod}\,[u'x' + u''x'' + \cdots + u^{(n)}x^{(n)}] \sim \text{mod}\,[v'y' + v''y'' + \cdots + v^{(n)}y^{(n)}],$$

und die Entwickelungen a. a. O. geben das Mittel, geeignete primitive Formen E und E' zu bestimmen. Das Product

$$(u'x' + u''x'' + \cdots + u^{(n)}x^{(n)}).\text{Fm}\,(v'y' + v''y'' + \cdots v^{(n)}y^{(n)})$$

muss nämlich durch $v'y' + v''y'' + \cdots + v^{(n)}y^{(n)}$ theilbar und der Quotient alsdann, ebenso wie die mit Fm bezeichnete Form, primitiv sein. So sind, um ein einfaches Beispiel aus der durch $\sqrt{-31}$ bezeichneten Species ganzer algebraischer Formen anzuführen, die drei Formen

$$5u + (2 + \sqrt{-31})u', \quad (1 + 3\sqrt{-31})v + (1 - 2\sqrt{-31})v', \quad 5w + (1 - 2\sqrt{-31})w'$$

einander absolut äquivalent. Nur die ersten beiden sind Grundformen der Species, die dritte gehört einer darin enthaltenen Species an; desshalb sind auch die Substitutions-Coefficienten bei den Transformationen der ersten beiden in einander und in die dritte gewöhnliche ganze Zahlen, aber bei der Transformation der dritten in eine der beiden ersten sind es ganze algebraische Zahlen der Species. In der That sind

$$\begin{matrix} u = -v + v' \\ u' = 3v - 2v' \end{matrix}, \quad \begin{matrix} v = 2u + u' \\ v' = 3u + u' \end{matrix}; \quad \begin{matrix} u = w + w' \\ u' = -2w' \end{matrix}, \quad \begin{matrix} w = u + 2(6 + \sqrt{-31})u' \\ w' = (4 - \sqrt{-31})u' \end{matrix}$$

die betreffenden Substitutionen, und die Gleichung

$$\frac{5u+(2+\sqrt{-31})u'}{5v+(1-2\sqrt{-31})v'} = \frac{5uv+(2+\sqrt{-31})u'v+(1+2\sqrt{-31})uv'-(12-\sqrt{-31}u'v')}{5v^2+2vv'+25v'^2}$$

legt den Quotienten der ersten und dritten Form als Quotienten von zwei primitiven Formen dar.

Die ganzen algebraischen *Zahlen* der Art $\mathfrak{S}$ und alle ihnen absolut äquivalenten Formen bilden die Hauptclasse derselben. Zwei Formen der Art $\mathfrak{S}$ sind einander relativ äquivalent, wenn sie, mit Formen der Hauptclasse multiplicirt, einander absolut äquivalent werden, d. h. also wenn sie sich im Sinne der absoluten Aequivalenz nur durch algebraische Zahlfactoren von einander unterscheiden. Im Sinne der relativen Aequivalenz verhalten sich also die Formen der Hauptclasse wie Einheiten (vgl. § 23, I'). Die Gesammtheit unter einander relativ äquivalenter Formen bildet je eine Formenclasse der Art $\mathfrak{S}$. Nach der zweiten, in § 23, II gegebenen Definition sind zwei Formen relativ äquivalent, wenn die *Verhältnisse* der Coefficienten je einer derselben in diejenigen der Coefficienten der anderen durch eine lineare Substitution mit ganzen algebraischen Zahlcoefficienten des Art-Bereichs ($\mathfrak{S}$) transformirbar sind. Wendet man diese Aequivalenz-Bestimmung auf die linearen Grundformen mit n Coefficienten an, so ergiebt sich als nothwendige und hinreichende Bedingung dafür, dass

$$u'x'+u''x''+\cdots+u^{(n)}x^{(n)} \quad \text{relat. aequ.} \quad v'y'+v''y''+\cdots+v^{(n)}y^{(n)}$$

ist, die Existenz einer Substitution

$$x':x'':\ldots:x^{(n)} = \sum_k c_{1k}y^{(k)} : \sum_k c_{2k}y^{(k)} : \ldots : \sum_k c_{nk}y^{(k)} \qquad (k=1,2,\ldots n),$$

bei welcher die n^2 Coefficienten c ganze Zahlen mit der Determinante Eins sind. Diese Aequivalenz-Bedingung ist besonders hervorzuheben, insofern eine völlig neue Auffassungs- und Behandlungsweise der ganzen algebraischen Zahlen eines bestimmten Art-Bereichs ($\mathfrak{S}$) darauf gegründet werden kann. Die ganze Theorie charakterisirt sich dann als eine solche der *Proportionen* von n Zahlen der festgesetzten Species, welche begrifflich in Systeme zusammen zu fassen sind. Ich beabsichtige in einer nächsten Abhandlung, in welcher ich die *speciellere* Theorie der ganzen algebraischen Zahlen entwickeln werde, auch auf diese Theorie der Proportionen näher einzugehen, und bemerke hier nur noch, dass ich durch meine Untersuchungen über die singulären Moduln der elliptischen Functionen zuerst auf den hier angegebenen Gesichtspunkt aufmerksam geworden bin; denn dort drängten sich

mir die (im Allgemeinen) gebrochenen, durch Gleichungen $ax^2+bx+c=0$ definirten algebraischen Zahlen x, also die Verhältnisse zweier ***ganzen*** algebraischen Zahlen bestimmter Art, als Gegenstand arithmetischer Behandlung auf, und zwar in der Weise, dass die Aequivalenz-Bestimmung zweier durch die Gleichungen $ax^2+bx+c=0$, $a_0x_0^2+b_0x_0+c_0=0$ erklärten algebraischen Zahlen x und x_0 mit derjenigen der quadratischen Formen (a, b, c), (a_0, b_0, c_0) übereinkommt.

Gemäss der ***dritten*** in § 23, III aufgestellten Definition sind zwei lineare Grundformen (von n Gliedern) relativ äquivalent, wenn sie nach Multiplication mit ganzen algebraischen Zahlen der Species $\mathfrak{S}$ durch lineare Substitutionen, deren Coefficienten gewöhnliche ganze Zahlen sind, in einander transformirt werden können. Diese Definition ist unmittelbar auf die zerlegbaren homogenen Formen n^{ten} Grades anzuwenden, welche aus den linearen Grundformen entstehen. Es seien nämlich

$$u'x'+u''x''+\cdots+u^{(n)}x^{(n)}, \quad v'y'+v''y''+\cdots+v^{(n)}y^{(n)}$$

einander relativ äquivalente lineare Grundformen der Species $\mathfrak{S}$; ferner seien x^0, y^0 ganze algebraische Zahlen der Species $\mathfrak{S}$, und es gehe

$$y^0(u'x'+u''x''+\cdots+u^{(n)}x^{(n)})$$

in

$$x^0(v'y'+v''y''+\cdots+v^{(n)}y^{(n)})$$

mittels einer Substitution

$$u^{(h)} = c_{h1}v'+c_{h2}v''+\cdots+c_{hn}v^{(n)} \qquad (h=1,2,\ldots n)$$

über, bei welcher die n^2 Substitutions-Coefficienten c_{hk} gewöhnliche ganze Zahlen mit der Determinante ***Eins*** sind, so dass die Gleichung

$$(A) \qquad y^0.\sum_h u^{(h)}x^{(h)} = x^0.\sum_k v^{(k)}y^{(k)} \qquad (h,k=1,2,\ldots n)$$

unter der Transformations-Bedingung

$$(B) \qquad u^{(h)}=\sum_k c_{hk}v^{(k)}, \quad |c_{hk}|=1 \qquad (h,k=1,2,\ldots n)$$

besteht. Wird nun in (A) auf beiden Seiten die Norm genommen und zur Abkürzung

$$\mathrm{Nm}\,x^0=X, \quad \mathrm{Nm}\,y^0=Y,$$

ferner gemäss den Bezeichnungen in § 14:

$$\mathrm{Nm}(u'x'+u''x''+\cdots+u^{(n)}x^{(n)}) = P.\mathrm{Fm}(u'x'+u''x''+\cdots+u^{(n)}x^{(n)}),$$
$$\mathrm{Nm}(v'y'+v''y''+\cdots+v^{(n)}y^{(n)}) = Q.\mathrm{Fm}(v'y'+v''y''+\cdots+v^{(n)}y^{(n)})$$

gesetzt, so resultirt die Gleichung

$$P.Y.\mathrm{Fm}(u'x'+u''x''+\cdots+u^{(n)}x^{(n)}) = Q.X.\mathrm{Fm}(v'y'+v''y''+\cdots+v^{(n)}y^{(n)}),$$

und es muss daher, da beide mit Fm bezeichneten Formen primitiv sind,

$$\mathrm{Fm}(u'x'+u''x''+\cdots+u^{(n)}x^{(n)}) = \mathrm{Fm}(v'y'+v''y''+\cdots+v^{(n)}y^{(n)})$$

sein, d. h. die eine dieser Formen muss in die andere durch die Substitution (B) übergehen. Die primitiven Formen

$$\mathrm{Fm}(u'x'+u''x''+\cdots+u^{(n)}x^{(n)})$$

sind nichts Anderes als die *„allgemeinen, in Linearfactoren zerlegbaren, homogenen ganzen ganzzahligen Formen mit einer ihrer Dimension gleichen Anzahl von Unbestimmten"*; es sind dies diejenigen Formen, welche bisher hauptsächlich für die Verallgemeinerung der binären quadratischen Formen ins Auge gefasst worden sind. Da jedoch die Theorie derselben aus derjenigen der linearen Grundformen unmittelbar resultirt, so charakterisirt sie sich nur als ein gewisser *Theil* der allgemeinen Theorie der *„ganzen algebraischen Formen"*. Aber diese Theorie hat nicht bloss den Vortheil grösserer Allgemeinheit für sich, sondern sie entspricht auch nicht minder den leitenden Gedanken der *Gauss*schen Einführung von Unbestimmten in die Arithmetik als denjenigen der *Kummer*schen Schöpfung der idealen Zahlen, und indem sie einerseits die Anwendung der unbestimmten Grössen überhaupt weiter entwickelt, andererseits die idealen Divisoren zu wirklichen algebraischen Ausdrücken mit unbestimmten Grössen umbildet, vermittelt sie die beiden „entgegengesetzten" Auffassungen der Theorie der zerlegbaren Formen und derjenigen der complexen Zahlen. Mit derselben Uebersichtlichkeit wie bei den *Kummer*schen idealen Zahlen lassen sich bei den ganzen algebraischen Formen alle aus der Compositions-Theorie hervorgehenden Resultate entwickeln, und ich habe dies schon in einer an Herrn *Schering*s Abhandlung über die Fundamentalclassen*) anknüpfenden Arbeit**) gezeigt, in welcher — nach der hier eingeführten Terminologie ausgedrückt — gewisse Beziehungen zwischen der Classenanzahl ganzer algebraischer Formen einer Gattung und derjenigen von Formen „enthaltener" Gattungen dargelegt sind. Aus denselben Principien lässt sich die einer elementareren Sphäre angehörige Bestimmung des Verhältnisses der Classenanzahlen für die verschiedenen Arten einer Gattung

*) „Die Fundamentalclassen der zusammensetzbaren arithmetischen Formen" von *Ernst Schering* (Abhandlungen d. Königl. Gesellsch. d. Wissensch. zu Göttingen, Bd. XIV, 1869).

**) Monatsbericht der Berliner Akad. d. Wissensch. 1. Dec. 1870.

herleiten, und zwar desshalb in so einfacher Weise, weil die zu den Fundamentalclassen der Haupt-Art $\mathfrak{S}$ bei irgend einer anderen Art $\bar{\bar{\mathfrak{S}}}$ hinzukommenden Classen nur Formen enthalten, welche Producte von primitiven Formen und von solchen ganzen algebraischen Zahlen der Haupt-Art $\mathfrak{S}$ sind, die sich in der Art $\bar{\bar{\mathfrak{S}}}$ nur als gebrochene Zahlen darstellen lassen.

Die verschiedene Dichtigkeit in verschiedenen Classen zerlegbarer Formen wird in der ersten *Kummer*schen Abhandlung mit Recht als ein wesentlicher Mangel der Theorie der zerlegbaren Formen gegenüber der Theorie der complexen Zahlen bezeichnet. Dieser Mangel rührt davon her, dass die Linearfactoren, welche als „ganze algebraische Formen" für sich zu behandeln sind, in den zerlegbaren Formen durch die Multiplication confundirt werden. Die ganzen algebraischen Formen haben also mit den *Kummer*schen idealen Zahlen auch den Vorzug gemein, dass ihre Dichtigkeit in jeder Classe dieselbe ist. Diese Vorbedingung eines sachgemässen Begriffes der Classenanzahl findet sich nämlich bei zerlegbaren Formen nicht erfüllt, wenn die conjugirten Linearfactoren nicht sämmtlich verschiedenen Gattungen angehören, und wenn die gewöhnliche (auf die lineare Transformation mit der Substitutions-Determinante Eins basirte) Aequivalenz-Bestimmung nicht modificirt wird. *Gauss* hat bei den quadratischen Formen eine solche Modification eingeführt, indem er die *„eigentliche* Aequivalenz" durch die Bedingung positiver Substitutions-Determinanten beschränkt; diese Weise der Beschränkung passt freilich nicht für Formen, welche mehr als zwei Unbestimmte enthalten, aber es lassen sich dann andere geeignete Beschränkungen aufstellen, und das massgebende Princip für die einzuführende Aequivalenz-Bestimmung ist,

> dass auf Grund derselben jede der Classen gleich dicht und ihre Anzahl möglichst klein werde.

Die ganzen algebraischen Formen haben endlich vor den zerlegbaren Formen das voraus, dass sie allen rationalen Rechnungsoperationen — nicht, wie diese, bloss dem in der Composition enthaltenen Multiplications-Verfahren — unterworfen werden können; sie können also, genau so wie gewöhnliche ganze Zahlen oder wie ganze Functionen von Variabeln, zu einander addirt, mit einander multiplicirt und auch durch einander dividirt werden, und wenn alsdann die Rechnungsresultate, d. h. die aus der Rechnung hervorgehenden Formen durch die ihnen absolut äquivalenten linearen Grundformen ersetzt werden, so tritt an die Stelle der Gleichheit die Aequivalenz.

§ 25.

Die Fundamentalgleichungen; die Discriminanten-Formen und ihre Divisoren der verschiedenen Stufen.

Wenn mit $x', x'', \dots x^{(n+m)}$, wie in § 8, die Elemente eines Fundamentalsystems der Art $\mathfrak{S}$ bezeichnet und die n Conjugirten jedes Elements durch untere Indices von einander unterschieden werden, so bilden die $n(n+m)$ ganzen algebraischen Grössen

$$x_i^{(k)} \qquad (i=1,2,\dots n;\ k=1,2,\dots n+m)$$

ein System, aus welchem das fundamentale System der Discriminanten hervorgeht, wenn man die verschiedenen Determinanten n^{ter} Ordnung des Systems $x_i^{(k)}$ bildet und jede derselben zum Quadrat erhebt. Nun ist schon a. a. O. eine „Form" gebildet worden, welche dieses Discriminanten-System vertritt, indem ein System von $m(m+n)$ „Unbestimmten"

$$x_h^{(k)} \qquad (h=n+1,n+2,\dots n+m;\ k=1,2,\dots n+m)$$

eingeführt und alsdann das Determinanten-Quadrat

$$|x_{k'}^{(k)}|^2 \qquad (k,k'=1,2,\dots n+m)$$

gebildet wurde. Es ist dies gemäss der Definition § 15, I eine ganze (rationale) Form des natürlichen Bereichs $[\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \dots]$ mit den $m(m+n)$ Unbestimmten $x_{n+1}^{(k)}, x_{n+2}^{(k)}, \dots x_{n+m}^{(k)}$, und diese kann durch jede ihr absolut äquivalente Form, z. B. auch durch eine lineare, ersetzt werden. Eine solche Form soll nunmehr als *„Discriminanten-Form* der Art $\mathfrak{S}$ oder des Art-Bereichs $(\mathfrak{S})$" bezeichnet werden; denn sie repräsentirt — wie die Darlegungen in § 8, verbunden mit den Entwickelungen in § 22, ergeben — den Complex der sämmtlichen Discriminanten des Art-Bereichs. Nämlich:

I. Die Discriminanten-Form ist der grösste gemeinschaftliche Theiler aller Discriminanten von je n ganzen algebraischen *Formen* des Art-Bereichs und als solcher dessen vollständige Invariante.

Wenn für einen Art-Bereich $(\mathfrak{S})$ ein Fundamentalsystem von nur n Elementen existirt, so gehört die Discriminanten-Form der Hauptclasse an, und an ihre Stelle tritt dann jene ganze rationale Form von $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \dots$, welche in § 8 „die Discriminante der Art" genannt worden ist.

Nach der im Anfange des vorigen Paragraphen aufgestellten Definition repräsentirt der Ausdruck

$$u'x' + u''x'' + \dots + u^{(n+m)}x^{(n+m)}$$

eine „lineare, eigentlich primitive Fundamentalform" mit den Unbestimmten u, und soll, weil er die Art $\mathfrak{S}$ repräsentirt, wenn an Stelle der Unbestimmten u ganze Grössen des natürlichen Bereichs $[\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots]$ treten, einfach mit $\mathfrak{S}$ bezeichnet werden. Wird das Product

$$\prod_i (x - u' x_i' - u'' x_i'' - \cdots - u^{(n+m)} x_i^{(n+m)}) \qquad (i = 1, 2, \ldots n)$$

mit $\mathfrak{F}(x)$ und das Product

$$\prod_h (x - u' x_h' - u'' x_h'' - \cdots - u^{(n+m)} x_h^{(n+m)}) \qquad (h = n+1, n+2, \ldots n+m),$$

in welchem die Grössen x_h, wie oben, $m(m+n)$ Unbestimmte bedeuten, mit $F(x)$ bezeichnet, so genügt jene mit $\mathfrak{S}$ bezeichnete eigentlich primitive Fundamentalform der Gleichung

$$\mathfrak{F}(\mathfrak{S}) = 0,$$

welche desshalb die *„Fundamentalgleichung* des Art-Bereichs $(\mathfrak{S})$" genannt werden soll.

Dem in § 8 aufgestellten Determinantensatze kann auf Grund der späteren Entwickelungen eine einfachere Fassung gegeben werden. Dort lautete nämlich der Satz so, dass die $n(n-1)^{\text{te}}$ Potenz der Determinante von n linearen Ausdrücken

$$\sum_k a_{ik} u_k \qquad (i, k = 1, 2, \ldots n)$$

eine lineare ganze homogene Function der Coefficienten Φ ist, welche bei der Entwickelung des Productes

$$\prod_{h,i} \left(\sum_k a_{hk} u_k - \sum_k a_{ik} u_k\right) \qquad (h, i, k = 1, 2, \ldots n;\ h \gtrless i)$$

auftreten. Da hiernach $|a_{ik}|^{n(n-1)}$ für das „Modulsystem" Φ congruent Null, also auch durch jede *Form* theilbar ist, deren Coefficienten die Elemente dieses Modulsystems sind, so ist

$$|a_{ik}|^{n(n-1)} \textit{ theilbar durch } \prod_{h,i} \left(\sum_k a_{hk} u_k - \sum_k a_{ik} u_k\right) \qquad (h, i, k = 1, 2, \ldots n),$$

im Sinne der absoluten Aequivalenz.

Die Discriminante der Gleichung $\mathfrak{F}(x) = 0$ ist ein Theiler der Discriminante der Gleichung $\mathfrak{F}(x) . F(x) = 0$, und diese wiederum, gemäss jenem Determinantensatze, wie er hier formulirt worden ist, ein Theiler von

$$|x_{k'}^k|^{n(n-1)} \qquad (k, k' = 1, 2, \ldots n).$$

Mit Benutzung des obigen Satzes I folgt also der Satz:

II. Für jeden Art-Bereich ist die Discriminante der Fundamentalgleichung ein Theiler der $\frac{1}{2}n(n-1)^{\text{ten}}$ Potenz der Discriminanten-Form, und enthält daher ausser der Discriminanten-Form selbst nur noch Theiler derselben.

Werden alle einzelnen Elemente des Fundamentalsystems $x', x'', x''', \ldots$ als ganze Functionen $(n-1)^{\text{ten}}$ Grades von $\mathfrak{S}$ ausgedrückt, so erscheinen die Coefficienten als Brüche, und zwar als ganze rationale Formen des Bereichs $[\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots]$, dividirt durch die Discriminante der Fundamentalgleichung. In der reducirten Gestalt haben diese Brüche also nur solche Nenner, welche Theiler der Discriminante der Fundamentalgleichung sind. Denkt man sich alle diese Nenner, welche ganze ganzzahlige Functionen der Variabeln $\mathfrak{R}$ und der Unbestimmten u sind, nach § 4 in ihre irreductibeln Factoren zerlegt, und dieselben in zwei Gruppen gesondert, von denen die eine die (eigentlich oder uneigentlich) primitiven *Formen* (mit den Unbestimmten u), die andere die rationalen *Grössen* des Bereichs $[\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots]$ umfasst, so kann die Discriminante der Fundamentalgleichung nur in *dem* Falle, nach Division durch die Discriminanten-Form, noch Theiler derselben enthalten, wenn überhaupt Factoren jener zweiten Gruppe vorkommen. Ist dies also nicht der Fall, so ist die Discriminante der Fundamentalgleichung der Discriminanten-Form äquivalent, wenigstens in jenem früheren weiteren Sinne, dass sich die eine von der anderen nur durch Factoren unterscheidet, welche (eigentlich oder uneigentlich) primitive Formen sind. Man findet aber leicht Beispiele von Art-Bereichen, für welche eine solche Aequivalenz nicht besteht, also die Discriminante der Fundamentalgleichung einzelne irreductible Divisoren der Discriminanten-Form, und zwar solche erster Stufe, in grösserer Anzahl enthält, als die Discriminanten-Form selbst. Anders verhält es sich bei der Haupt-Art, welche nunmehr allein betrachtet werden soll.

Sind $x', x'', \ldots x^{(n+m)}$ die Elemente des Fundamentalsystems der Haupt-Art $\mathfrak{S}$ oder der Gattung $\mathfrak{G}$, so soll die lineare eigentlich primitive Fundamentalform

$$u'x' + u''x'' + \cdots + u^{(n+m)}x^{(n+m)},$$

weil sie alle ganzen algebraischen Grössen der Gattung repräsentirt, mit $\mathfrak{G}$ bezeichnet werden. Wird nun für eine Variable $\mathfrak{R}$

$$\mathfrak{F}(\mathfrak{R}) = \prod_i (\mathfrak{R} - u'x'_i - u''x''_i - \cdots - u^{(n+m)}x_i^{(n+m)}) \qquad (i=1, 2, \ldots n)$$

gesetzt, die Discriminante der Gleichung $\mathfrak{F}(\mathfrak{R}) = 0$ mit $\mathfrak{D}$ und das Determinanten-Quadrat

$$|x_{k'}^{k}|^2 \qquad (k, k'=1, 2, \ldots n)$$

mit D bezeichnet, so soll

$\mathfrak{F}(\mathfrak{R}) = 0$ die „Fundamentalgleichung *der Gattung*",

$\mathfrak{D}$ die „Discriminante der Fundamentalgleichung *der Gattung*" und

D die „Discriminanten-Form *der Gattung*"

genannt werden. Nach dem obigen Satze I ist alsdann D der grösste gemeinschaftliche Theiler aller Discriminanten der Gattung, also auch ein Theiler von $\mathfrak{D}$, und nach dem Satze II ist $\mathfrak{D}$ wiederum ein Theiler von $D^{\frac{1}{2}n(n-1)}$. Bedeutet nun $\mathfrak{H}$ eine ganze algebraische Form, welche aus der Form $\mathfrak{G}$ entsteht, wenn die Unbestimmten $u', u'', \ldots$ durch $v', v'', \ldots$ ersetzt werden, unterscheidet man ferner die Conjugirten von $\mathfrak{G}$ und $\mathfrak{H}$, den conjugirten Werthen der Elemente x entsprechend, durch untere Indices von einander, so ist

$$\mathfrak{H}_i - \mathfrak{H}_k = \sum_h v^{(h)}(x_i^{(h)} - x_k^{(h)}) \qquad (h = 1, 2, \ldots n+m).$$

Dieser Ausdruck stellt eine ganze algebraische Form dar, welche nach § 17, II durch den algebraischen Divisor

$$\operatorname{mod}[\sum_h u^{(h)}(x_i^{(h)} - x_k^{(h)})] \quad \text{oder} \quad \operatorname{mod}[\mathfrak{G}_i - \mathfrak{G}_k] \qquad (h = 1, 2, \ldots n+m)$$

theilbar ist, und nach der in § 14 eingeführten Bezeichnungsweise ist daher

$$\frac{\mathfrak{H}_i - \mathfrak{H}_k}{\mathfrak{G}_i - \mathfrak{G}_k} \operatorname{Fm}(\mathfrak{G}_i - \mathfrak{G}_k)$$

eine ganze algebraische Form. Demgemäss ist auch

$$\operatorname{Fm}(\mathfrak{G}_i - \mathfrak{G}_k) . \sum_k \frac{\mathfrak{H}_i - \mathfrak{H}_k}{\mathfrak{G}_i - \mathfrak{G}_k} \qquad (k = 1, 2, \ldots i-1, i+1, \ldots n)$$

eine ganze algebraische Form und zwar von der Gattung $\mathfrak{G}_i$. Denkt man sich $\mathfrak{H}$ als ganze Function $(n-1)^{\text{ten}}$ Grades von $\mathfrak{G}$ dargestellt, so erscheinen, wie oben erwähnt, die Coefficienten als Brüche mit Nennern, deren irreductible Factoren dort in zwei Gruppen gesondert worden sind. Die Factoren der ersten Gruppe, welche in den Nennern vorkommen, können nun, da sie primitive Formen sind, weggeschafft werden, wenn $\mathfrak{H}$ mit einer dazu erforderlichen primitiven Form multiplicirt wird. Nachdem dies geschehen, mögen alle diejenigen Glieder der Form weggelassen werden, in welchen die Coefficienten der Potenzen von $\mathfrak{G}$ *ganz* sind. Ist alsdann $\mathfrak{G}^m$ die höchste Potenz von $\mathfrak{G}$, welche in der resultirenden Form, die mit $\mathfrak{H}^0$ bezeichnet werden möge, vorkommt, so ist der Coefficient von $\mathfrak{G}^m$ ein Bruch, dessen Nenner N, da er nur Factoren jener zweiten Gruppe enthält, eine Grösse des Bereichs $[\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots]$ ist. Derselbe Coefficient bildet aber, multi-

plicirt mit $(n-m)$, den Coefficienten von $\mathfrak{G}^{m-1}$, d. h. der höchsten Potenz von $\mathfrak{G}$, in der Form

$$\mathrm{Fm}(\mathfrak{G}_i-\mathfrak{G}_k).\sum_k \frac{\mathfrak{H}_i^0-\mathfrak{H}_k^0}{\mathfrak{G}_i-\mathfrak{G}_k} \qquad (k=1,2,\ldots i-1, i+1,\ldots n),$$

und wenn also der Nenner N nicht eine in $(n-m)$ enthaltene Zahl ist, so kann aus dieser Form auf die angegebene Weise eine neue gebildet werden, welche in Beziehung auf $\mathfrak{G}$ nur vom $(m-2)^{\text{ten}}$ Grade ist. Solche Formen können aber nicht von beliebig kleinem Grade m existiren, namentlich nicht solche, für welche $m=0$ ist, und es ergiebt sich demnach, dass, wenn die mit $x', x'', \ldots$ bezeichneten Elemente der Form $\mathfrak{H}$ als ganze Functionen von $\mathfrak{G}$ dargestellt werden, in den Coefficienten als Nenner nur eigentlich primitive Formen und solche Factoren der Discriminanten-Form auftreten können, welche uneigentlich primitive Formen mit den Unbestimmten u oder ganze Zahlen aus der Reihe $2, 3, \ldots n-2$ sind. Diese Zahlenreihe kann noch weiter beschränkt werden, aber statt hierauf näher einzugehen, soll die wichtigere Bemerkung angefügt werden, dass diese Zahlenreihe und demnach die zweite Alternative überhaupt wegfällt, wenn die Gattung $\mathfrak{G}$ keine Conjugirte hat, also eine *Galois*sche Gattung ist. In diesem Falle kann nämlich die Form

$$\frac{\mathfrak{H}_i^0-\mathfrak{H}_k^0}{\mathfrak{G}_i-\mathfrak{G}_k}\mathrm{Fm}(\mathfrak{G}_i-\mathfrak{G}_k)$$

selbst, weil sie alsdann ebenfalls zur Gattung $\mathfrak{G}$ gehört, an Stelle der oben daraus gebildeten Summe, zur Reduction verwendet werden, und wenn man diese aus $\mathfrak{H}^0$ gebildete Form mit $\mathfrak{H}'$ bezeichnet, dann aus $\mathfrak{H}'$ ebenso eine Form $\mathfrak{H}''$ u. s. w. bildet, so reducirt sich $\mathfrak{H}^{(m)}$ einfach auf den Coefficienten, welcher in $\mathfrak{H}^0$ mit $\mathfrak{G}^m$ multiplicirt ist. Da dieser Coefficient hiernach eine ganze rationale Grösse des Bereichs sein muss, so kann ein Nenner N der zweiten Gruppe überhaupt nicht vorkommen. Die vorstehende Deduction stimmt ihrem wesentlichen Inhalte nach mit derjenigen überein, welche ich in § 5 meiner Abhandlung „über die Discriminante algebraischer Functionen einer Variabeln*)“ gegeben habe; aber mit Hülfe der in der vorliegenden Arbeit enthaltenen Entwickelungen konnte die Darstellung vereinfacht und der Kern der Sache bloss gelegt werden. Die Deduction zeigt,

---

*) Journal für Mathematik, Bd. 91, S. 301 sqq.

III. dass für irgend eine Gattung $\mathfrak{G}$ die Discriminante der Fundamentalgleichung $\mathfrak{D}$ entweder mit der Discriminanten-Form der Gattung D im Sinne der vollständigen absoluten Aequivalenz (§ 22, X^0) übereinstimmt oder doch, in demselben Sinne der Aequivalenz, ausser D selbst nur noch solche Divisoren von D enthalten kann, welche Formen höherer als erster Stufe oder — falls die Gattung $\mathfrak{G}$ Conjugirte hat — Zahlen aus der Reihe $2, 3, \ldots n-2$ sind.

Ob in Wirklichkeit solche überflüssigen Zahlentheiler in der Discriminante der Fundamentalgleichung vorkommen, habe ich noch nicht ermitteln können; ich habe mich vergeblich bemüht ein Beispiel dafür aufzufinden, habe aber ebensowenig vermocht das Gegentheil zu beweisen. Jene Beschränkung ist also vielleicht unnöthig; im Wesentlichen hat das aus dem obigen (III) abzuleitende fernere Resultat,

IV. dass die gesammte arithmetische Theorie der algebraischen Grössen auf eine Theorie der ganzen ganzzahligen Functionen von Variabeln und Unbestimmten zurückgeführt werden kann,

seine Geltung; es ist für die früher allein betrachteten Divisoren erster Stufe auch von jeder Einschränkung zu befreien, und weil es auf diese angewendet und an denselben näher erläutert werden soll, möge es hiermit specieller formulirt werden:

IV^0. Die arithmetische Theorie der algebraischen Grössen eines durch $(\mathfrak{G}, \mathfrak{R}', \mathfrak{R}'', \ldots \mathfrak{R}^{(n-1)})$ bezeichneten Gattungs-Bereichs ist durch die Theorie der ganzen rationalen *„Formen“* eines natürlichen Rationalitäts-Bereichs von $\mathfrak{n}$ Variabeln $(\mathfrak{R}^0, \mathfrak{R}', \ldots \mathfrak{R}^{(n-1)})$ zu ersetzen, und zwar so, dass dabei an die Stelle der jenem Gattungs-Bereich angehörigen ganzen ***algebraischen*** Formen $\mathfrak{m}^{ter}$ Stufe diejenigen ganzen ***rationalen*** Formen dieses natürlichen Rationalitäts-Bereichs treten, deren Stufenzahl $\mathfrak{m}+1$ ist.

Einzig und allein die Formen höherer als erster Stufe, welche Factoren der Discriminanten-Form von $\mathfrak{G}$ sind, würden da, wo die obige zweite Alternative eintritt, eine besondere Behandlung (z. B. ein Zurückgehen auf eine höhere Gattung) erfordern; für die Formen erster Stufe aber soll jene principiell wichtige Reduction vom Algebraischen auf das Rationale hier vollständig dargelegt werden.

Es bedeute $\mathfrak{F}(\mathfrak{R}) = 0$, wie oben, die Fundamentalgleichung der durch $\mathfrak{G}$ bezeichneten Gattung, so dass $\mathfrak{F}(\mathfrak{G}) = 0$ wird; es sei ferner P eine irre-

ductible ganze rationale Function der Variabeln $\mathfrak{R}'$, $\mathfrak{R}''$, $\mathfrak{R}'''$, ..., also eine Grösse des Rationalitäts-Bereichs $[\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots]$, und es sei endlich mit $F(\mathfrak{R})$ irgend eine ganze Function von $\mathfrak{R}$, deren Coefficienten Grössen desselben Bereichs $[\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots]$ sind, d. h. also eine ganze ganzzahlige Function von $\mathfrak{R}$, $\mathfrak{R}'$, $\mathfrak{R}''$, $\mathfrak{R}'''$, ... bezeichnet. Alsdann lässt sich die nothwendige und hinreichende Bedingung dafür, dass

$$\mathrm{Nm}\, F(\mathfrak{G}) \equiv 0 \quad (\mathrm{mod.}\, P)$$

sei, dadurch ausdrücken, dass die beiden Formen

$$P + \mathfrak{v}\mathfrak{F}(\mathfrak{R}), \quad P + vF(\mathfrak{R})$$

einen gemeinschaftlichen Theiler zweiter Stufe haben. Ist dies nämlich nicht der Fall, so kann die Resultante der Elimination von $\mathfrak{R}$ aus $\mathfrak{F}(\mathfrak{R})$ und $F(\mathfrak{R})$ nicht durch P theilbar sein, und da dieselbe in der Form

$$\Phi(\mathfrak{R})F(\mathfrak{R}) + \Psi(\mathfrak{R})\mathfrak{F}(\mathfrak{R})$$

dargestellt werden kann, so ist sie auch gleich $\Phi(\mathfrak{G})F(\mathfrak{G})$. Die Norm dieses Products $\mathrm{Nm}\,\Phi(\mathfrak{G}).\mathrm{Nm}\,F(\mathfrak{G})$ ist also die n^{te} Potenz der Resultante und folglich $\mathrm{Nm}\,F(\mathfrak{G})$ nicht durch P theilbar. Wenn aber andererseits jene beiden Formen einen gemeinsamen Theiler zweiter Stufe haben, so muss wenigstens einer der irreductibeln Factoren von $P + \mathfrak{v}\mathfrak{F}(\mathfrak{R})$ in $P + vF(\mathfrak{R})$ enthalten sein. Die erstere der beiden Formen ist eine Form zweiter Stufe, und ihre irreductibeln Factoren sind, wie nachher (S. 117) gezeigt werden soll, sämmtlich von einander verschieden. Wird von Formen höherer als zweiter Stufe abgesehen, d. h. werden diese äquivalent Eins angenommen, so wie es bei den algebraischen Divisoren in §§ 14 sqq. schon mit den Formen zweiter Stufe geschah, so lässt sich die Zerlegung durch folgende Aequivalenz darstellen:

$$(A) \qquad P + \mathfrak{v}\mathfrak{F}(\mathfrak{R}) \sim (P + \mathfrak{v}_1\mathfrak{F}_1(\mathfrak{R}))(P + \mathfrak{v}_2\mathfrak{F}_2(\mathfrak{R}))\ldots,$$

und es ist hiernach die auf alle Wurzeln der Gleichung $\mathfrak{F}_1(\mathfrak{R}) = 0$ bezogene Norm von $\mathfrak{F}(\mathfrak{R})$ durch P theilbar. Diese Norm ist ihrem absoluten Werthe nach mit $\mathrm{Nm}\,\mathfrak{F}_1(\mathfrak{G})$ identisch, so dass die Congruenz

$$(B) \qquad \mathrm{Nm}(P + \mathfrak{v}_1\mathfrak{F}_1(\mathfrak{G})) \equiv 0 \quad (\mathrm{mod.}\, P)$$

besteht. Die Voraussetzung, dass die Form $P + \mathfrak{v}\mathfrak{F}(\mathfrak{R})$ in $P + vF(\mathfrak{R})$ enthalten sei, hat demnach in der That die Congruenz

$$\mathrm{Nm}(P + vF(\mathfrak{G})) \equiv 0 \quad (\mathrm{mod.}\, P)$$

und also schliesslich auch die Congruenz

$$\mathrm{Nm}\, F(\mathfrak{G}) \equiv 0 \quad (\mathrm{mod.}\, P)$$

zur Folge. — Die obige Zerlegung der Form $P + \mathfrak{v}\,\mathfrak{F}(\mathfrak{R})$ in irreductible Formen zweiter Stufe kann aus der Zerlegung der Congruenz $\mathfrak{F}(\mathfrak{R}) \equiv 0\ (\mathrm{mod.}\, P)$ in ihre $(\mathrm{mod.}\, P)$ irreductibeln Factoren hergeleitet werden. Wird nämlich eine solche Zerlegung durch die Congruenz

$$(C) \qquad \mathfrak{F}(\mathfrak{R}) \equiv f_1(\mathfrak{R})^{n_1} f_2(\mathfrak{R})^{n_2} \dots \quad (\mathrm{mod.}\, P)$$

dargestellt, in welcher unter den Functionen $f_1(\mathfrak{R}),\ f_2(\mathfrak{R}), \dots$ irreductible, im Sinne der Congruenz modulo P, zu verstehen sind, so bedeutet diese Congruenz nichts Anderes als eine Gleichung

$$(C') \qquad \mathfrak{F}(\mathfrak{R}) = f_1(\mathfrak{R})^{n_1} f_2(\mathfrak{R})^{n_2} \cdots + P.\bar{\mathfrak{F}}(\mathfrak{R}).$$

Da $\mathfrak{F}(\mathfrak{R})$ irreductibel ist, so kann der grösste gemeinschaftliche Theiler von $\bar{\mathfrak{F}}(\mathfrak{R})$ und $f_1(\mathfrak{R})^{n_1}$, im Sinne der Congruenz modulo P, nur eine Potenz von $f_1(\mathfrak{R})$ sein, deren Exponent kleiner als n_1 ist, und die Zerlegung von $\bar{\mathfrak{F}}(\mathfrak{R})$ liefert daher eine Gleichung

$$\bar{\mathfrak{F}}(\mathfrak{R}) = f_1(\mathfrak{R})^{m_1} f_2(\mathfrak{R})^{m_2} \cdots + P.\bar{\bar{\mathfrak{F}}}(\mathfrak{R}),$$

in welcher $n_1 > m_1,\ n_2 > m_2, \dots$ ist. Zerlegt man hier wieder $\bar{\bar{\mathfrak{F}}}(\mathfrak{R})$ und führt dann in derselben Weise fort, so gelangt man schliesslich zu einer Gleichung, in welcher die mit P multiplicirte Function von $\mathfrak{R}$, im Sinne der Congruenz modulo P, keinen der Factoren $f_1(\mathfrak{R}),\ f_2(\mathfrak{R}), \dots$ mehr enthält. Für einen dieser Factoren z. B. für $f_1(\mathfrak{R})$ resultirt daher eine Gleichung

$$(D) \qquad \mathfrak{F}(\mathfrak{R}) = f_1(\mathfrak{R})^{n_1} \varphi(\mathfrak{R}) + P f_1(\mathfrak{R})^{m_1} \varphi_1(\mathfrak{R}) + P^2 f_1(\mathfrak{R})^{l_1} \varphi_2(\mathfrak{R}) + \cdots + P^r \varphi_r(\mathfrak{R}),$$

in welcher $\varphi_r(\mathfrak{R})$, nach dem Modul P betrachtet, keinen Factor mit $\mathfrak{F}(\mathfrak{R})$ gemein hat, also $\mathrm{Nm}\, \varphi_r(\mathfrak{G})$ nicht durch P theilbar ist, und in welcher überdies die Bedingungen

$$n_1 \geqq r, \quad m_1 \geqq r-1, \quad l_1 \geqq r-2, \dots$$

erfüllt sind. Wenn nun in der Gleichung (D) für die Variable $\mathfrak{R}$ der Werth $\mathfrak{G}$ substituirt wird, so resultirt eine Gleichung für den Bruch

$$\frac{P}{f_1(\mathfrak{G})} \mathrm{Nm}\, \varphi_r(\mathfrak{G}),$$

welche denselben als *ganze* algebraische Form charakterisirt, und da dieser Bruch auch als ein solcher mit dem Nenner P dargestellt werden kann,

so folgt, dass P ein Theiler der Discriminanten-Form und zwar, da P eine ganze rationale Grösse des Bereichs ist, zur zweiten Gruppe gehörig sein muss. Nach dem obigen Satze (III) existiren aber solche Theiler nicht, ausser etwa — falls die Gattung $\mathfrak{G}$ Conjugirte hat — Zahlen aus der Reihe 2, 3, ... $n-2$. Wenn ferner P nicht Theiler der Discriminanten-Form und also auch nicht Theiler der Discriminante der Fundamentalgleichung ist, so ist überhaupt keiner der Exponenten n_1, n_2, ... in der Congruenz (C) grösser als Eins. Es ergiebt sich also aus vorstehender Entwickelung, dass — abgesehen von dem Falle, wo P eine der Zahlen 2, 3, ... $n-2$ und zugleich Theiler der Discriminanten-Form ist, und wo überdies die Gattung $\mathfrak{G}$ Conjugirte hat — stets

> die durch die Gleichung (C^0) definirte Function $\bar{\mathfrak{F}}(\mathfrak{R})$, im Sinne der Congruenz modulo P, relativ prim gegen die Function $\mathfrak{F}(\mathfrak{R})$ und daher $\mathrm{Nm}\,\bar{\mathfrak{F}}(\mathfrak{G})$ nicht durch P theilbar ist.

Das hier entwickelte Resultat begründet die vollkommene Regularität der durch die Congruenz (C) oder durch die Gleichung (C') dargestellten Zerlegung der Congruenz $\mathfrak{F}(\mathfrak{R}) \equiv 0 \pmod{P}$ in ihre irreductibeln Factoren. Es ergiebt sich daraus unmittelbar die Zerlegung von P in die irreductibeln algebraischen Divisoren der Gattung $\mathfrak{G}$, auf welche im Anfange des § 18 (S. 60) hingewiesen worden ist, nämlich

$$(A^0) \qquad P \sim \mathrm{mod}\,[P+\mathfrak{v}_1 f_1(\mathfrak{G})]^{n_1} . \mathrm{mod}\,[P+\mathfrak{v}_2 f_2(\mathfrak{G})]^{n_2} \ldots,$$

so wie auch die Zerlegung der Form zweiter Stufe $P+\mathfrak{v}\mathfrak{F}(\mathfrak{R})$ in ihre irreductibeln Factoren:

$$(A') \qquad P+\mathfrak{v}\mathfrak{F}(\mathfrak{R}) \sim (P+\mathfrak{v}_1 f_1(\mathfrak{R})^{n_1})(P+\mathfrak{v}_2 f_2(\mathfrak{R})^{n_2})\ldots,$$

und es ist also in jener Aequivalenz (A)

$$\mathfrak{F}_1(\mathfrak{R}) = f_1(\mathfrak{R})^{n_1}, \quad \mathfrak{F}_2(\mathfrak{R}) = f_2(\mathfrak{R})^{n_2}, \ldots$$

zu nehmen. Hieraus ist auch, wenn $F(\mathfrak{R})$, wie oben, irgend eine ganze ganzzahlige Function von $\mathfrak{R}, \mathfrak{R}', \mathfrak{R}'', \ldots$ bedeutet, die Zerlegung der Formen

$$(E) \qquad F(\mathfrak{R})+\mathfrak{v}\mathfrak{F}(\mathfrak{R})$$

(wie bei (A), im Sinne der Aequivalenz) herzuleiten. Unter den irreductibeln Formen zweiter Stufe, welche bei Fixirung von $\mathfrak{F}(\mathfrak{R})$ als Factoren der unendlich vielen Formen (E) auftreten, bilden diejenigen die Hauptclasse (im Sinne der relativen durch Fixirung von $\mathfrak{F}(\mathfrak{R})$ bedingten Aequivalenz, genau übereinstimmend mit der in § 23, I gegebenen Definition), welche unter

den Formen (E) selbst vorkommen, also aus zwei Gliedern bestehen, deren eines $\mathfrak{F}(\mathfrak{R})$ selbst zum Coefficienten hat. Im Uebrigen sind es nämlich Formen $P + \mathfrak{v}_k f_k(\mathfrak{R})^{n_k}$, welche die irreductibeln Factoren der Formen (E) bilden.

Es ist wohl zu beachten, dass die Formen zweiter Stufe $P + \mathfrak{v}_k f_k(\mathfrak{R})^{n_k}$, auch wenn $n_k > 1$ ist, irreductibel sind. Die Zerlegung (A') der Formen $P + \mathfrak{v}\,\mathfrak{F}(\mathfrak{R})$ ergiebt also, wie oben (S. 114) schon im Voraus erwähnt worden ist, stets ungleiche irreductible Factoren; aber bei der Zerlegung (A'') von P in algebraische Divisoren kommen dann und nur dann Divisoren mehrfach vor, wenn P ein irreductibler Factor der Discriminanten-Form ist. Ist dies nämlich nicht der Fall, so sind — wie schon oben (S. 116) hervorgehoben worden — die Zahlen $n_1, n_2, \ldots$ sämmtlich nur gleich Eins. Wenn andererseits P Factor der Discriminanten-Form ist, so muss wenigstens eine der Zahlen grösser als Eins sein, weil dann die Function $\mathfrak{F}(\mathfrak{R})$ mit ihrer nach $\mathfrak{R}$ genommenen Ableitung, im Sinne der Congruenz modulo P, einen gemeinsamen Theiler hat. Der hier bewiesene Satz kann dahin formulirt werden,

> dass von den sämmtlichen irreductibeln ganzen rationalen Grössen eines Bereichs $[\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots]$ nur alle diejenigen, welche Theiler der Discriminanten-Form der Gattung $\mathfrak{G}$ sind, irreductible algebraische Divisoren der Gattung mehrfach enthalten.

Für den Fall, wo die Gattung $\mathfrak{G}$ Conjugirte hat, kann der Satz ohne Weiteres aus der Geltung des Satzes für eine die Gattung $\mathfrak{G}$ enthaltende ***Galois***sche Gattung erschlossen werden.

Tritt an Stelle eines beliebigen Rationalitäts-Bereichs $[\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots]$ der absolute der gewöhnlichen ganzen Zahlen, so ist P Primzahl und die oben eingeführte Grösse $\mathfrak{R}$ die einzige Variable; es existiren also keine Formen höherer als zweiter Stufe, und jene Zerlegung (A') der Form zweiter Stufe $P + \mathfrak{v}\mathfrak{F}(\mathfrak{R})$ in ihre irreductibeln Factoren gilt also im Sinne der vollständigen absoluten Aequivalenz (§ 22, X^0): Der Sache nach stimmt jene Zerlegung mit derjenigen der Congruenz $\mathfrak{F}(\mathfrak{R}) \equiv 0 \pmod{P}$ überein, und die Benutzung ***dieser*** für die Zerlegung (A^0) einer Primzahl P in ihre algebraischen Primtheiler oder (nach der ***Kummer***schen Ausdrucksweise) in ihre idealen Primfactoren ist ebenso einfach als natürlich. Wie schon in § 19 (S. 69) erwähnt, habe ich gleich im Anfange meiner Beschäftigung mit der Theorie der algebraischen Zahlen den Versuch gemacht, die Theorie der höheren Congruenzen dafür zu benutzen, und wenn man von den Factoren der Discriminante absieht, so gelingt dies auch in der elementarsten und leichtesten

Weise. Denn bei der Uebertragung der *Kummer*schen Definition der idealen Zahlen auf ganzzahlige Functionen einer Wurzel einer ganzzahligen Gleichung $\varphi(x) = 0$ handelt es sich nur darum, für die Coefficienten einer ganzen ganzzahligen Function $\psi(x)$ die linearen Congruenz-Bedingungen aufzustellen, unter denen die Eliminations-Resultante von $\varphi(x)$ und $\psi(x)$ durch eine Primzahl p theilbar wird; offenbar müssen aber dann $\varphi(x)$ und $\psi(x)$, modulo p betrachtet, einen gemeinsamen Theiler haben, und jene Congruenz-Bedingungen bestehen also einfach darin, dass $\psi(x)$ irgend einen der modulo p irreductibeln Factoren von $\varphi(x)$, im Sinne einer Congruenz modulo p, als Theiler enthalten muss. Es ist dies fast nur eine andere Einkleidung jener elementaren Resultate, welche in der schon in § 21 (S. 80) citirten *Schönemann*schen Abhandlung*) entwickelt sind. Ganz anders verhält es sich aber, wenn die Primfactoren der Discriminante mit in Betracht gezogen werden. Ein Versuch, auch diese in einer Theorie mit zu umfassen, welche auf jener beschränkten Darstellungsweise der complexen Zahlen (als ganze Functionen einer einzigen ganzen algebraischen Zahl) aufgebaut ist, liegt in der *Zolotareff*schen Arbeit vor, die im neusten Bande des *Resal*schen Journals veröffentlicht ist. Dieser Versuch ist aber, wie ich glaube, verfehlt; und nach den von *Zolotareff* im Eingange seiner Arbeit citirten *Dedekind*schen Publicationen aus dem Jahre 1871, in welchen mit voller Klarheit und Schärfe die Nothwendigkeit dargethan ist, jene beschränkte Grundlage der complexen Zahlentheorie aufzugeben, musste ein Versuch, dieselbe dennoch beizubehalten, von vorn herein, als der Natur der Sache widersprechend, aussichtslos erscheinen. Nicht bei irgend einer speciellen Gleichung einer Gattung algebraischer Zahlen, sondern nur bei der *Fundamentalgleichung*, deren Bildung sich einerseits auf die Construction des Fundamentalsystems und andererseits auf die Association der „Formen" stützt, ist jene Anknüpfung an die Theorie der höheren Congruenzen von Erfolg. Da in dem hier betrachteten Falle des absoluten Rationalitäts-Bereichs die Discriminanten-Form einer gewöhnlichen ganzen Zahl äquivalent ist, so kann diese selbst unter D verstanden werden, und der Quotient $\frac{\mathfrak{D}}{D}$ ist alsdann eine primitive Form mit den Unbestimmten u, welche nur, falls die Gattung $\mathfrak{G}$ Conjugirte hat, noch mit Potenzen von Primfactoren von D, die kleiner als $n-1$ sind, multiplicirt sein kann. Ist dies wirklich der Fall, so hat natürlich auch die

*) Journal f. Mathematik Bd. 31, S. 269.

Discriminante jeder speciellen Zahlengleichung der Gattung $\mathfrak{G}$ dieselben überflüssigen Factoren, aber auch wenn es nicht der Fall und der Quotient $\frac{\mathfrak{D}}{D}$ also nur eine primitive Form ohne Zahlenfactor ist, kann dieselbe doch für alle ganzzahligen Werthe der Unbestimmten u einen und denselben Theiler enthalten; denn dies tritt z. B. ein (vgl. § 8 am Schlusse, S. 25), wenn die primitive Form sich als ganze homogene Function von lauter Ausdrücken $u^p - u$ darstellen lässt und p Primzahl ist. Ein solcher Fall liegt bei einer von Herrn *Dedekind* angegebenen Gattung algebraischer Zahlen vor, die durch die kubische Gleichung $\alpha^3 - \alpha^2 - 2\alpha - 8 = 0$ definirt wird*). Hierbei ist, wenn u eine Unbestimmte bedeutet, $\alpha + \frac{4u}{\alpha}$ Wurzel einer Fundamentalgleichung, und deren Discriminante enthält ausser D nur das Quadrat der primitiven Form $2u^3 + u^2 + u - 2$, welche allerdings für alle ganzzahligen Werthe von u durch 2 theilbar wird. Ich selbst habe bei meiner ersten Beschäftigung mit dieser Theorie im Jahre 1858 ein ähnliches Beispiel bei den dreizehnten Wurzeln der Einheit gefunden. Diese Beispiele zeigen eben nur, dass die Association der Formen nicht bloss in der allgemeinen Theorie der algebraischen Grössen, sondern selbst in der specielleren der algebraischen Zahlen der Natur der Sache entspricht. Doch darf hier nicht unerwähnt bleiben, dass merkwürdiger Weise auch bei dieser elementareren Frage der Darstellung der complexen Zahlen, ganz analog wie bei der höheren Frage der Darstellung ihrer Primtheiler, eine zweite Art der Association, nämlich die von algebraischen Zahlen höherer Ordnung, zu demselben Ziele führt. In der That sieht man leicht, dass die Unbestimmten jener primitiven Form, welche eine Wurzel der Fundamentalgleichung darstellt, stets als ganze *algebraische* Zahlen dem angegebenen Zwecke gemäss bestimmt werden können, und wenn man z. B. oben für u eine dritte Wurzel der Einheit setzt, so wird die primitive Form ihrem absoluten Werthe nach gleich Eins.

Kommen im Rationalitäts-Bereich überhaupt Variable $\mathfrak{R}$ vor, so enthält die Discriminanten-Form stets Formen höherer Stufen als mehrfache

*) *R. Dedekind*, „Ueber den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Congruenzen." Abhandlungen der Königl. Gesellschaft der Wissensch. zu Göttingen. Bd. 23, S. 30.

Theiler; sie bilden „die Singularitäten“ der Discriminanten-Form, deren Untersuchung das grösste Interesse aber auch wohl grosse Schwierigkeiten bietet. Um so mehr ist es hervorzuheben, dass in einer von Herrn *Netto* neuerdings veröffentlichten Arbeit*), welche die algebraischen Probleme ebenfalls, wie es hier geschehen, im Geiste der Arithmetik behandelt, schon eine Reihe von Resultaten jener Art entwickelt sind. Um deren Bedeutung für die allgemeine Theorie der algebraischen Grössen darzulegen, muss ich an die aus einem Rationalitäts-Bereich $(\mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n)$ hervorgehenden Gattungen anknüpfen, welche den Gegenstand der Erörterungen des § 12 bilden. Die ganzen algebraischen Grössen dieser Gattungen sind ganze Functionen der Variabeln $x_1, x_2, \ldots x_n$ und also algebraische Functionen der mit $\mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n$ bezeichneten elementaren symmetrischen Functionen derselben n Variabeln x. In jeder dieser Gattungen existiren Fundamentalsysteme von nur ebenso viel Elementen, als die Ordnung der Gattung beträgt (vgl. § 12, S. 39), und diese Ordnung ist oben (§ 12, S. 35), wie auch a. a. O. von Herrn *Netto*, mit ϱ bezeichnet worden. An die Stelle der Discriminanten-Form tritt demnach **) eine „Discriminante der Gattung“, und diese ist eine Potenz der Discriminante der Gleichung

$$x^n - \mathfrak{f}_1 x^{n-1} + \mathfrak{f}_2 x^{n-2} - \cdots \pm \mathfrak{f}_n = 0,$$

deren Exponent in der *Netto*schen Arbeit bestimmt wird. Die Discriminante jeder einzelnen Gleichung der Gattung ist durch diese Discriminante der Gattung theilbar, und überdies enthält, wie von Herrn *Netto* gezeigt wird, jede der Gleichungs-Discriminanten (nach der hier angenommenen Terminologie) noch Divisoren-Systeme oder Formen höherer Stufe als Theiler, welche zugleich mehrfache Theiler der Discriminanten-Form selbst sind. Wenn diese *Netto*schen Resultate sich, wie es mir wahrscheinlich ist, auch für die hier eingeführte Fundamentalgleichung verwenden lassen, so würden sie Beiträge zur Erkenntniss jener primitiven Form $\frac{\mathfrak{D}}{D}$ (namentlich in Bezug auf ihre Divisoren höherer Stufe) liefern, welche einen Hauptgegenstand der obigen Entwickelungen (vgl. den Satz III) bildet.

Für einen natürlichen Rationalitäts-Bereich von $\mathfrak{n}-1$ Variabeln $(\mathfrak{R}', \mathfrak{R}'', \ldots \mathfrak{R}^{(\mathfrak{n}-1)})$ repräsentirt eine bestimmte Gattung algebraischer Grössen

*) *E. Netto*, „Zur Theorie der Discriminanten“. Journal f. Mathematik, Bd. 90, S. 164.

**) Vgl. den oben (S. 108) an den Satz I angeschlossenen Zusatz.

insofern eine (n−1)-fache Mannigfaltigkeit, als jedem System reeller Werthe der n−1 Variabeln 𝔑 eine Gattung algebraischer Grössenwerthe 𝔊 entspricht. Das Gleichungssystem, welches dadurch entsteht, dass die Discriminanten-Form D gleich Null gesetzt wird, definirt den „Ort" derjenigen Punkte der (n−1)-fachen Mannigfaltigkeit 𝔑, für welche alle Elemente des Fundamentalsystems und daher *alle* Grössen der Gattung mit conjugirten zusammenfallen, wo also der Gattungsbegriff eigentlich aufhört. Dieser Ort ist im Allgemeinen eine (n−2)-fache Mannigfaltigkeit, aber es können auch „isolirte" Mannigfaltigkeiten geringerer Ausdehnung dazu gehören, wie ich schon an dem Beispiele der durch biquadratische Gleichungen definirten Gattungen gezeigt habe *). Die Mannigfaltigkeiten geringerer Ausdehnung werden von denjenigen Punkten 𝔑 erfüllt, für welche mehr als zwei conjugirte Reihen von Elementen des Fundamentalsystems, z. B. also drei Reihen oder zwei Paare von Reihen, mit einander identisch werden, und alle diese besonderen Mannigfaltigkeiten bilden die „Singularitäten" jener gesammten durch $D = 0$ repräsentirten (n−2)-fachen Mannigfaltigkeit. Die für irgend eine Gattung 𝔊 — also allgemeiner als für eine einzelne *Gleichung* — zu bildenden *Sturm*schen Reihen haben keine andere Bestimmung als die weitere Sonderung der durch die (n−2)-fache Mannigfaltigkeit $D = 0$ von einander abgetrennten (n−1)-fach ausgedehnten Gebiete, gemäss der Anzahl reeller oder complexer Reihen conjugirter Elemente des Fundamentalsystems, und da diese Gebietstheile nur durch jene Singularitäten von einander geschieden sind, so ist für die Bildung einer *Sturm*schen Reihe ganzer rationaler Functionen der Variabeln 𝔑 allein der Gesichtspunkt massgebend, dass sie, gleich Null gesetzt, (n−2)-fache Mannigfaltigkeiten darstellen sollen, welche bestimmte von jenen Singularitäten enthalten und im Uebrigen mit der Mannigfaltigkeit $D = 0$ nichts gemeinsam haben. *Die ganze theoretische Bedeutung der Sturmschen Reihen geht hiernach in jenen „Singularitäten der Discriminantenform" vollständig auf* **); und diese Singularitäten selbst

*) Vgl. meine beiden im Monatsbericht der Berliner Akademie vom Febr. 1878 veröffentlichten Mittheilungen, in denen überhaupt den obigen verwandte Entwickelungen gegeben sind.

**) Es ist wohl zu unterscheiden zwischen dem ursprünglichen, klassischen *Sturm*schen *Verfahren* und den später so viel behandelten *Sturm*schen Reihen oder Functionen. Jenes Verfahren bewährt sich gerade auch in denjenigen Entwickelungen, welche über den beschränkten Standpunkt der *Sturm*schen Reihen hinaus führen. (Vgl. meine citirte Mittheilung im Monatsbericht d. Berl. Akademie vom Febr. 1878 S. 149.)

sind — von jenen Hülfsmitteln der Anschauung losgelöst und rein arithmetisch aufgefasst — nichts Anderes als

V. ***die in der Discriminantenform als mehrfache Theiler enthaltenen Formen höherer Stufe.***

Aber diese arithmetische Auffassung greift in derselben Weise über jene „geometrische" hinaus wie in § 22 XIII⁰ (S. 92) bei der Zerlegung einer Form in ihre irreductibeln Factoren, wenn hier wie dort unter den Formen auch solche vorkommen, die für keinerlei Werthsysteme der Variabeln $\mathfrak{R}$ gleich Null werden und sich also der bildlichen geometrischen Darstellung entziehen. Dass aber gerade auch derartige Formen, unter diesen auch reine ***Zahlen,*** als Discriminanten-Theiler wirklich vorkommen und von wesentlicher Bedeutung sein können, dafür habe ich bei meinen arithmetischen Untersuchungen über die singulären Moduln ein Beispiel in den Gleichungen gefunden, von denen die Theilung der elliptischen Functionen mit unbestimmten Moduln abhängt.

Der eigentliche Ausgangspunkt für die vorliegende arithmetische Behandlung der algebraischen Grössen wurde in § 3 durch die Einschränkung der allgemeinsten Rationalitäts-Bereiche gewonnen; aber es mussten dabei die Gattungs-Bereiche noch neben den natürlichen in Betracht gezogen werden. Gleich nach Einführung der Gattungen wurden alsdann in § 8 die charakteristischen Invarianten derselben in den fundamentalen Systemen der Discriminanten ermittelt; aber der dortige Standpunkt gestattete noch keinen Einblick in ihren ganz verschiedenartigen Inhalt. Wenn jetzt in diesem Schlussparagraphen oben (IV) die weitere Einschränkung der Rationalitäts-Bereiche und hier (V) die Erkenntniss der verschiedenen Stufen der in der Discriminanten-Form enthaltenen Divisoren dargelegt werden konnte, so hat die arithmetische Theorie der algebraischen Grössen, indem sie in ihrer weiteren Entwickelung zur grösstmöglichen Vereinfachung und vollständigsten Klärung der eigenen Grundlagen geführt hat, ihre innere Wahrheit und Folgerichtigkeit dargethan.

De unitatibus complexis.

Dissertatio inauguralis arithmetica *).

In principalia doctrinae numerorum incrementa introductionem numerorum complexorum, ipsi summo huius scientiae creatori debitam, referendam esse inter omnes constat. Qui numeri quam vim ad promovendam scientiam habeant, inde elucet, quod arcte et cum residuis potestatum et cum theoria formarum altiorum graduum et cum circuli sectione cohaerent. Summus *Gauss* primus disquisitiones de numeris complexis formae $a+b\sqrt{-1}$ in publicum edidit, quarum theoriam postea Cl. *Lejeune-Dirichlet* uberius tractavit **). Generalioris numerorum complexorum speciei mentionem fecit Cl. *Jacobi*, qui circuli sectionem pertractans in hanc quaestionem incidit ***). Praeterea ad hanc partem doctrinae numerorum spectant et observatio Cli. *Jacobi* †) et recentiore tempore disputatio Cli. *Kummer* „de numeris complexis qui unitatis radicibus et numeris integris realibus constant," et commentatio Illi. *Eisenstein* „de formis cubicis trium variabilium etc." ††). — Ex quo prospectu, quam pauca de numeris complexis huc usque in publicum edita sint, iam elucet, ideoque in sequentibus praecipue tantum ad illam Cli. *Kummer* disputationem lectorem reiicere potero. Cum vero nonnulla theoremata in illa commentatione iam tradita elegantius demonstrare mihi contigerit, etiamque alia quaedam nondum tradita ad perscrutandas unitates complexas adhibenda sint, cumque denique, quoad nunc possim,

*) Haec dissertatio aestate anni MDCCCXLV ordini philosophorum universitatis Berolinensis proposita eique ex auctoritate summi viri *Lejeune-Dirichlet* probata est. Typis autem tum non excusa est nisi pars aliqua, scilicet paragraphi 1—16, quae publice prodiit d. X. m. Septembris a. MDCCCXLV; quae sequuntur paragraphi 17—20 ineditae adhuc nunc primum evulgantur.

**) *Crelles* Journal Bd. 24.

***) Monatsberichte der Berliner Akademie, 1837 (S. 127 sqq.); v. etiam commentationem Illi. *Eisenstein*. „Beiträge zur Kreistheilung" (*Crelles* Journal Bd. 27).

†) *Crelles* Journal Bd. 19 S. 314. ††) *Crelles* Journal Bd. 28.

totum aliquod conficere velim, disquisitionem fere ab initio repetere praeferam. Quem ad finem pars prior huius dissertationis, unitatibus complexis deditae, illas disquisitiones numerorum complexorum quasi fundamentales continebit.

Denique adnotandum recentissimo tempore Clum. *Lejeune-Dirichlet*, dum in Italia versabatur, quaestiones de unitatibus principales ratione maxime generali latissimeque patente mira quidem simplicitate tractavisse, quarum rerum prospectum nunc in publicum editurus est. Quod quidem cum acciperem his meis disquisitionibus iam finitis, eas elaborare tamen non plane inutile videbatur, et quia hae quae proferentur methodi ab illis methodis generalibus omnino differunt, et quia in pertractandis unitatibus ex unitatis radicibus compositis quaestiones quaedam se offerunt, quas ipsas tanquam speciales alicuius momenti esse arbitror.

PARS PRIOR.

§ 1.

Ne postea investigationum ordinem interrumpere oporteat, hoc quod sequitur lemma, cuius frequens erit usus et quo nonnullae demonstrationes praecidentur, antea praemittimus.

Sint aequationis algebraicae n^{ti} gradus coefficientibus integris (coefficiens ipsius x^n sit unitas) n radices: α, β, γ etc. atque eiusdem aequationis, si tanquam congruentiam modulo p (ubi p numerus primus) consideres, n radices: a, b, c etc.; sit porro $f(\alpha, \beta, \gamma, \ldots)$ functio radicum algebraica integra symmetrica, congruentiam

$$f(\alpha, \beta, \gamma, \ldots) \equiv f(a, b, c, \ldots) \pmod{p}$$

locum habere dico.

Dem. Etenim quamque functionem radicum algebraicam integram symmetricam *identice* tanquam functionem integram expressionum: $\alpha+\beta+\gamma+\cdots$, $\alpha\beta+\alpha\gamma+\cdots$ etc. repraesentari posse constat. Ergo $f(a, b, c, \ldots)$ eadem functio integra expressionum: $a+b+\cdots$, $ab+ac+\cdots$ etc., quae $f(\alpha, \beta, \gamma, \ldots)$ ipsarum $\alpha+\beta+\gamma+\cdots$, $\alpha\beta+\alpha\gamma+\cdots$ etc. sit oportet. Cum vero $a+b+c+\cdots$ coefficienti ipsius x^{n-1} i. e. quantitati $\alpha+\beta+\gamma+\cdots$ pariterque $ab+ac+\cdots$

ipsi $\alpha\beta + \alpha\gamma + \cdots$ etc. secundum modulum p congrua esse notum est, id quod contendimus facile concludi potest.

Nunc sit ν numerus primus, ω radix aequationis $\omega^\nu = 1$ primitiva, sint porro ε, ε_1, ... $\varepsilon_{\lambda-1}$ periodi radicum ω, quarum quaeque μ terminos contineat, ita ut habeamus $\lambda\mu = \nu - 1$ et:

$$
\text{(I.)} \quad \begin{cases}
\varepsilon \;\;= \omega + \omega^{g^\lambda} + \omega^{g^{2\lambda}} + \cdots + \omega^{g^{(\mu-1)\lambda}}, \\
\varepsilon_1 = \omega^g + \omega^{g^{\lambda+1}} + \omega^{g^{2\lambda+1}} + \cdots + \omega^{g^{(\mu-1)\lambda+1}}, \\
\quad \vdots \qquad \vdots \qquad \vdots \\
\varepsilon_{\lambda-1} = \omega^{g^{\lambda-1}} + \omega^{g^{2\lambda-1}} + \omega^{g^{3\lambda-1}} + \cdots + \omega^{g^{\mu\lambda-1}},
\end{cases}
$$

ubi g est radix primitiva ipsius ν. Ex quibus aequationibus statim colligitur:

$$\varepsilon_{\varkappa\lambda+r} = \varepsilon_r \quad \text{et} \quad 1 + \varepsilon + \varepsilon_1 + \cdots + \varepsilon_{\lambda-1} = 0.$$

Iam posito

$$a\varepsilon + a_1\varepsilon_1 + a_2\varepsilon_2 + \cdots + a_{\lambda-1}\varepsilon_{\lambda-1} = f(\varepsilon)\,^{*}),$$

ubi literis: $a, a_1, \ldots a_{\lambda-1}$ numeri reales integri designantur, talem expressionem $f(\varepsilon)$ numerum complexum voco. Iam quia omnis periodorum functio rationalis tanquam omnium periodorum functio linearis repraesentari potest, productum numerorum complexorum rursum in formam ipsius $f(\varepsilon)$ redigi posse patet. Deinde eadem, qua Cl. ***Kummer*** in disputatione illa iam laudata (§ 1) usus est ratione, ex aequatione:

$$a\varepsilon + a_1\varepsilon_1 + \cdots + a_{\lambda-1}\varepsilon_{\lambda-1} = b\varepsilon + b_1\varepsilon_1 + \cdots + b_{\lambda-1}\varepsilon_{\lambda-1}$$

sequitur, ut sint $a = b$, $a_1 = b_1$, ... $a_{\lambda-1} = b_{\lambda-1}$.

Numeri $f(\varepsilon_1)$, $f(\varepsilon_2)$, ... $f(\varepsilon_{\lambda-1})$ numero $f(\varepsilon)$ coniuncti dicuntur et facile, brevitatis causa $f(\varepsilon) = f$, $f(\varepsilon_1) = f_1$ etc. positis, aequationes sequentes locum habere elucet:

$$
\text{(II.)} \quad \begin{cases}
a\varepsilon + a_1\varepsilon_1 + \cdots + a_{\lambda-1}\varepsilon_{\lambda-1} = f, \\
a\varepsilon_1 + a_1\varepsilon_2 + \cdots + a_{\lambda-1}\varepsilon \;\;\;= f_1, \\
\quad \vdots \qquad \vdots \qquad \vdots \\
a\varepsilon_{\lambda-1} + a_1\varepsilon + \cdots + a_{\lambda-1}\varepsilon_{\lambda-2} = f_{\lambda-1}.
\end{cases}
$$

Quod aequationum systema ut secundum quantitates a, a_1, ... solvamus, litera α aliquam aequationis $\alpha^\lambda = 1$ radicem designamus. Tum aequatione prima in 1, secunda in α, tertia in α^2 etc. postrema in $\alpha^{\lambda-1}$ ductis iisque additis aequationem:

---

*) Cum illa periodorum functio linearis eadem tanquam functio ipsius ε rationalis integra repraesentari possit.

$$\text{(III.)}\quad \begin{aligned}&(\varepsilon+\varepsilon_1\alpha+\varepsilon_2\alpha^2+\cdots+\varepsilon_{\lambda-1}\alpha^{\lambda-1})(a+a_1\alpha^{-1}+a_2\alpha^{-2}+\cdots+a_{\lambda-1}\alpha^{-(\lambda-1)})\\ &\qquad = f+f_1\alpha+f_2\alpha^2+\cdots+f_{\lambda-1}\alpha^{\lambda-1}\end{aligned}$$

pro quaque unitatis radice λ^{ta} α obtinemus.

Cum vero expressio $\varepsilon+\varepsilon_1\alpha+\cdots+\varepsilon_{\lambda-1}\alpha^{\lambda-1}$ nihil aliud sit, nisi id quod Cl. *Jacobi* in commentatione illa iam supra laudata*) signo $F(\alpha)$ denotat, formulam l. c. traditam in auxilium vocamus:

$$(\varepsilon+\varepsilon_1\alpha+\cdots+\varepsilon_{\lambda-1}\alpha^{\lambda-1})(\varepsilon+\varepsilon_1\alpha^{-1}+\cdots+\varepsilon_{\lambda-1}\alpha^{-(\lambda-1)}) = \nu\,.\,\alpha^{\frac{1}{2}(\nu-1)} = \nu\,.\,\alpha^{\frac{1}{2}\mu\lambda},$$

quae pro quoque ipsius α valore, excepto illo $\alpha=1$, locum habet. Qua adhibita atque aequatione (III) per ipsum $\varepsilon+\varepsilon_1\alpha^{-1}+\varepsilon_2\alpha^{-2}+\cdots+\varepsilon_{\lambda-1}\alpha^{-(\lambda-1)}$ multiplicata aequatio:

$$\text{(IV.)}\quad \begin{aligned}&\nu(a+a_1\alpha^{-1}+a_2\alpha^{-2}+\cdots+a_{\lambda-1}\alpha^{-(\lambda-1)})\\ &\quad = (f+f_1\alpha+\cdots+f_{\lambda-1}\alpha^{\lambda-1})\,.\,(\varepsilon+\varepsilon_1\alpha^{-1}+\cdots+\varepsilon_{\lambda-1}\alpha^{-(\lambda-1)})\end{aligned}$$

(posito μ numerum esse parem) oritur, atque pro quoque ipsius α valore unitate excepta valet. Unde concludi licet:

$$\text{(V.)}\quad \begin{cases}\nu a = f\varepsilon+f_1\varepsilon_1+f_2\varepsilon_2+\cdots+f_{\lambda-1}\varepsilon_{\lambda-1}+m,\\ \nu a_1 = f\varepsilon_1+f_1\varepsilon_2+f_2\varepsilon_3+\cdots+f_{\lambda-1}\varepsilon+m,\\ \quad\vdots\qquad\qquad\vdots\qquad\qquad\vdots\\ \nu a_{\lambda-1} = f\varepsilon_{\lambda-1}+f_1\varepsilon+f_2\varepsilon_1+\cdots+f_{\lambda-1}\varepsilon_{\lambda-2}+m.\end{cases}$$

Quando enim pro quibusvis quantitatibus b et c systema aequationum habemus:

$$\begin{aligned}&b+b_1\alpha+\cdots+b_r\alpha^r+\cdots+b_{\lambda-1}\alpha^{\lambda-1} = c+c_1\alpha+\cdots+c_r\alpha^r+\cdots+c_{\lambda-1}\alpha^{\lambda-1},\\ &b+b_1\alpha^2+\cdots+b_r\alpha^{2r}+\cdots+b_{\lambda-1}\alpha^{2(\lambda-1)} = c+c_1\alpha^2+\cdots+c_r\alpha^{2r}+\cdots+c_{\lambda-1}\alpha^{2(\lambda-1)},\\ &\qquad\vdots\qquad\qquad\vdots\qquad\qquad\vdots\\ &b+b_1\alpha^{\lambda-1}+\cdots+b_r\alpha^{(\lambda-1)r}+\cdots+b_{\lambda-1}\alpha = c+c_1\alpha^{\lambda-1}+\cdots+c_r\alpha^{(\lambda-1)r}+\cdots+c_{\lambda-1}\alpha,\end{aligned}$$

facile prima aequatione in α^{-r}, secunda in α^{-2r} etc. ducta iisque additis aequatio colligitur:

$$\lambda b_r-(b+b_1+\cdots+b_{\lambda-1}) = \lambda c_r-(c+c_1+\cdots+c_{\lambda-1})\quad\text{seu}\quad b_r = c_r+m,$$

ubi m respectu r constans est.

Ut quantitas m definiatur, adnotamus istis aequationibus ν additis fieri:

$$\text{(VI.)}\quad \nu(a+a_1+\cdots+a_{\lambda-1}) = (f+f_1+\cdots+f_{\lambda-1})(\varepsilon+\varepsilon_1+\cdots+\varepsilon_{\lambda-1})+\lambda m.$$

Cum vero $\varepsilon+\varepsilon_1+\cdots+\varepsilon_{\lambda-1}=-1$ sit et $a+a_1+\cdots+a_{\lambda-1}=-(f+f_1+\cdots+f_{\lambda-1})$ esse ex aequatione (III) ibi ponendo $\alpha=1$ colligatur, aequatio (VI) mutatur in:

*) Monatsberichte der Berliner Akademie 1837 (S. 128).

$$-(\nu-1)(f+f_1+\cdots+f_{\lambda-1})=\lambda m \quad \text{seu} \quad -\mu(f+f_1+\cdots+f_{\lambda-1})=m.$$

Quo valore ipsius m substituto has consequimur aequationes, systemata (II) et (V) repraesentantes:

$$\text{(VII.)} \quad \begin{cases} f_r = a\varepsilon_r + a_1\varepsilon_{r+1}+\cdots+a_{\lambda-1}\varepsilon_{r-1}, \\ -\nu a_r = f(\mu-\varepsilon_r)+f_1(\mu-\varepsilon_{r+1})+\cdots+f_{\lambda-1}(\mu-\varepsilon_{r-1}) \end{cases}$$

pro ipsius r valoribus: $0,\ 1,\ 2,\ \ldots\ \lambda-1$.

Iam vero respecta analogia numerorum complexorum, qui radicibus unitatis ad numeros compositos (ν) pertinentibus constant, numeros complexos $f(\varepsilon)$ sub hac forma accipere convenit, scilicet:

$$f(\varepsilon) = a+a_1\varepsilon+a_2\varepsilon^2+\cdots+a_{\lambda-1}\varepsilon^{\lambda-1},$$

quamquam *unitates* complexas in posterum illius formae supra exhibitae ponemus. — Productum talium numerorum $f(\varepsilon)$ rursus in eandem formam redigi posse inde elucet, quod quaevis periodus tanquam functio rationalis integra unius repraesentari potest, quodque quaevis functio integra periodi ε per aequationem illam gradus λ^{ti}, quarum radices $\varepsilon,\ \varepsilon_1,\ \ldots\ \varepsilon_{\lambda-1}$ sunt, ad gradum $(\lambda-1)^{\text{tum}}$ redigi potest. Denique ex aequalitate duorum numerorum complexorum aequalitatem singulorum coefficientium colligi posse inde patet, quod functio periodi integra gradus $(\lambda-1)^{\text{ti}}$ evanescere nequit, nisi omnes eius coefficientes evanescunt.

Productum omnium numerorum coniunctorum, tanquam functio periodorum invariabilis integra, numerus realis integer est atque norma appellatur. Est igitur:

$$f(\varepsilon)f(\varepsilon_1)\ldots f(\varepsilon_{\lambda-1}) = \operatorname{Nm} f(\varepsilon)$$

et quidem respectu ε. Quodsi enim $f(\varepsilon)$ tanquam functio alius periodi e. g. ipsius ω consideratur, ita ut sit: $f(\varepsilon)=\varphi(\omega)$, apparet esse

$$\operatorname{Nm}\varphi(\omega)=\varphi(\omega)\varphi(\omega_1)\ldots\varphi(\omega_{\nu-2}) \quad \text{sive} \quad \operatorname{Nm}\varphi(\omega)=(\operatorname{Nm}f(\varepsilon))^{\mu}.$$

Neque unquam, ne ex aequalitate signorum ambiguitas oriatur, verendum est. Caeterum ex ipsa definitione colliguntur aequationes:

$$\operatorname{Nm}f(\varepsilon)=\operatorname{Nm}f(\varepsilon_r) \quad \text{et} \quad \operatorname{Nm}(f(\varepsilon).\varphi(\varepsilon))=\operatorname{Nm}f(\varepsilon).\operatorname{Nm}\varphi(\varepsilon).$$

Cum sit

$$(\operatorname{Nm}f(\varepsilon))^{\mu}=\operatorname{Nm}\varphi(\omega)\equiv 1 \pmod{\nu},$$

posito numerum $\operatorname{Nm}f(\varepsilon)$ ad ipsum ν primum esse (Disput. Cli. *Kummer* § 2), sequitur, ut quaevis norma respectu ε residuum sit λ^{tae} potestatis modulo ν.

§ 2.

Ponatur p numerus primus eiusmodi, ut sit $p^{\mu} \equiv 1 \pmod{\nu}$, atque sit:

$$p = p(\varepsilon)p(\varepsilon_1)\ldots p(\varepsilon_{\lambda-1}) = \mathrm{Nm}\,p(\varepsilon),$$

istos factores ulterius in factores complexos ex his ipsis periodis ε compositos discerpi non posse atque inter se diversos esse, eadem qua Cl. ***Kummer*** in disputatione sua (§ 5) usus est ratione probatur. Deinde cum nuper a Clo. ***Kummer*** demonstratum sit, congruentiam λ^{ti} gradus:

$$(x-\varepsilon)(x-\varepsilon_1)\ldots(x-\varepsilon_{\lambda-1}) \equiv 0 \pmod{p}$$

semper habere λ radices, si p condicioni sufficit $p^{\mu} \equiv 1 \pmod{\nu}$ *), has ipsas designemus literis: $e, e_1, \ldots e_{\lambda-1}$ **). Iam haec duo habentur theoremata:

1. Si $f(\varepsilon)$ numerus est complexus, cuius norma per numerum primum p divisibilis est, unus numerorum $f(e), f(e_1), \ldots$ secundum modulum p nihilo congruus erit; et quando unus numerorum $f(e)$ ipsum p metitur, etiam $\mathrm{Nm} f(\varepsilon)$ factorem p implicat.

Dem. Cum productum $f(\varepsilon)f(\varepsilon_1)\ldots f(\varepsilon_{\lambda-1})$ functio sit algebraica integra symmetrica radicum aequationis $(x-\varepsilon)(x-\varepsilon_1)\ldots(x-\varepsilon_{\lambda-1}) = 0$, secundum primum nostrum lemma erit:

$$f(\varepsilon)f(\varepsilon_1)\ldots f(\varepsilon_{\lambda-1}) \equiv f(e)f(e_1)\ldots f(e_{\lambda-1}) \pmod{p}$$

$$\text{sive } \mathrm{Nm} f(\varepsilon) \equiv f(e)f(e_1)\ldots f(e_{\lambda-1}) \pmod{p},$$

unde theoremata illa sponte manant.

2. ***Theorema.*** Sint $p(\varepsilon), p(\varepsilon_1), \ldots$ factores primi complexi numeri primi p sitque $p(e)$ ille factor, qui condicionem explet $p(e) \equiv 0 \pmod{p}$, congruentia haec locum habebit:

$$e \equiv \varepsilon \pmod{p(\varepsilon)}.$$

Dem. Ponatur

$$(e-\varepsilon)\,p(\varepsilon_1)p(\varepsilon_2)\ldots p(\varepsilon_{\lambda-1}) = \varphi(\varepsilon),$$

unde

$$(e-\varepsilon_1)\,p(\varepsilon)p(\varepsilon_2)\ldots p(\varepsilon_{\lambda-1}) = \varphi(\varepsilon_1) \text{ etc.;}$$

tum erit $\varphi(e) = 0$ et $\varphi(e_1) \equiv \varphi(e_2) \equiv \cdots \equiv \varphi(e_{\lambda-1}) \equiv 0 \pmod{p}$, quia omnes hi numeri factorem $p(e)$ implicant, quem nihilo congruum supposuimus. Iam erit secundum illud lemma:

$$\varphi(\varepsilon)+\varphi(\varepsilon_1)+\cdots+\varphi(\varepsilon_{\lambda-1}) \equiv \varphi(e)+\varphi(e_1)+\cdots+\varphi(e_{\lambda-1}) \equiv 0 \pmod{p}.$$

---

*) In commentatione „de divisoribus formarum quarundam etc.“ quae proximo tempore edetur; vel etiam in commentatione Cli. *Schoenemann* (*Crelles* Journal, Bd. 19, S. 306).

**) Adnotamus quodvis e_r eandem ipsius e functionem integram esse quam ε_r ipsius ε.

Deinde erit $\varphi(\varepsilon)^2+\varphi(\varepsilon)\varphi(\varepsilon_1)+\cdots+\varphi(\varepsilon)\varphi(\varepsilon_{\lambda-1})\equiv\varphi(\varepsilon)^2$, cum reliqua producta omnes factores $p(\varepsilon)$ ideoque ipsum p contineant. Ergo habemus: $\varphi(\varepsilon)^2\equiv 0\ (\text{mod.}p)$. Iam si p ad ν primum supponitur, erit $p^{\nu-1}\equiv 1\ (\text{mod.}\nu)$ atque (cf. § 3, 1)

$$\varphi(\varepsilon)^{p^{\nu-1}}\equiv\varphi(\varepsilon^{p^{\nu-1}})\equiv\varphi(\varepsilon)\ (\text{mod.}p).$$

Erit autem

$$\varphi(\varepsilon)^{p^{\nu-1}}=\varphi(\varepsilon)^{p^{\nu-1}-2}.\varphi(\varepsilon)^2\equiv 0\ (\text{mod.}p),$$

unde denique:

$\varphi(\varepsilon)\equiv 0\ (\text{mod.}p)$, i. e. $(e-\varepsilon)p(\varepsilon_1)p(\varepsilon_2)\ldots p(\varepsilon_{\lambda-1})\equiv 0\ (\text{mod.}p(\varepsilon)p(\varepsilon_1)\ldots p(\varepsilon_{\lambda-1}))$, ergo:

$$e-\varepsilon\equiv 0\ (\text{mod.}p(\varepsilon)).$$

Casu $p=\nu$ habemus $\text{Nm}\,p(\varepsilon)=\nu$ et posito $p(\varepsilon)=f(\omega)$ erit $\text{Nm}\,f(\omega)=(\text{Nm}\,p(\varepsilon))^\mu$, ergo $\text{Nm}\,f(\omega)\equiv 0\ (\text{mod.}\nu^\mu)$. Eaque de re $f(1)\equiv 0\ (\text{mod.}\nu)$ (disputatio Cli. ***Kummer*** § 2); ergo cum sit $(1-\omega)(1-\omega^2)\cdots=\nu$, erit quoque $f(1)\equiv 0\ (\text{mod.}(1-\omega))$. Deinde propter congruentiam $1\equiv\omega\ (\text{mod.}(1-\omega))$ habemus $f(\omega)\equiv 0\ (\text{mod.}(1-\omega))$.

Iam posito $\qquad f(\omega)=(1-\omega)f'(\omega)$ erit $\text{Nm}\,f'(\omega)\equiv 0\ (\text{mod.}\nu^{\mu-1})$,

ergo sicut supra $\qquad f'(\omega)=(1-\omega)f''(\omega)$.

Qua ratione denique obtinemus $f(\omega)=(1-\omega)^\mu\varphi(\omega)$. Est vero

$$\text{Nm}\,f(\omega)=\nu^\mu=\nu^\mu\,\text{Nm}\,\varphi(\omega),$$

unde $\varphi(\omega)$ unitatem complexam esse patet. Ergo erit quoque:

$$(1-\omega)^\mu\equiv 0\ (\text{mod.}f(\omega))\ \text{seu}\ (\text{mod.}p(\varepsilon)).$$

Deinde cum simili modo e congruentia $\text{Nm}(e-\varepsilon)\equiv 0\ (\text{mod.}\nu)$ colligatur

$$(e-\varepsilon)=(1-\omega)^\mu\psi(\omega)\quad\text{sive}\quad(e-\varepsilon)\equiv 0\ (\text{mod.}(1-\omega)^\mu),$$

denique respecta congruentia illa: $(1-\omega)^\mu\equiv 0\ (\text{mod.}p(\varepsilon))$ habebitur:

$$e-\varepsilon\equiv 0\ (\text{mod.}p(\varepsilon)).$$

3. ***Theorema.*** Si duo habentur factores primi complexi non coniuncti eiusdem numeri primi p e. g. $p(\varepsilon)$ et $p^1(\varepsilon)$, singuli factores $p^1(\varepsilon)$ e singulis $p(\varepsilon)$ multiplicando per unitates complexas deducuntur *).

Dem. Sint $p(e)$ et $p^1(e)$ factores per ipsum p divisibiles, erit:

$$p^1(e)\equiv 0\ (\text{mod.}p)\ \text{ideoque etiam}\ (\text{mod.}p(\varepsilon)).$$

Est vero $e\equiv\varepsilon\ (\text{mod.}p(\varepsilon))$, unde $p^1(\varepsilon)\equiv 0\ (\text{mod.}p(\varepsilon))$ i. e. $p^1(\varepsilon)=p(\varepsilon).\varphi(\varepsilon)$, ubi $\varphi(\varepsilon)$ unitas complexa est, quia $\text{Nm}\,p^1(\varepsilon)=p=\text{Nm}\,p(\varepsilon).\text{Nm}\,\varphi(\varepsilon)=p.\text{Nm}\,\varphi(\varepsilon)$, ergo $\text{Nm}\,\varphi(\varepsilon)=1$.

*) Quod theorema casus tantum specialis theorematis 2 in § 3 est.

4. ***Theorema.*** Quando norma numeri complexi $p(\varepsilon)$ numerus primus p est ab ipso ν diversus, unum tantum numerorum $p(e)$ numerus p metiri potest.

Dem. Sit $p(e) \equiv p(e_r) \equiv 0$ (mod. p) ergo $p(e_r) \equiv 0$ (mod. $p(\varepsilon)$). Deinde cum habeamus $e \equiv \varepsilon$ et $e_r \equiv \varepsilon_r$ (mod. $p(\varepsilon)$)*), sequitur, ut sit:

$$p(\varepsilon_r) \equiv 0 \text{ (mod. } p(\varepsilon)) \text{ sive } p(\varepsilon_r) = p(\varepsilon).\varphi(\varepsilon).$$

Ergo cum sit: $p(\varepsilon).p(\varepsilon_1)\ldots p(\varepsilon_{\lambda-1}) \equiv 0$ (mod. p), etiam erit:

$$\varphi(\varepsilon).p(\varepsilon).p(\varepsilon_1)\ldots p(\varepsilon_{\lambda-1}) = p(\varepsilon_r)^2.p(\varepsilon_1)\ldots p(\varepsilon_{r-1})p(\varepsilon_{r+1})\cdots \equiv 0 \text{ (mod. } p)$$

etiamque

$$p(\varepsilon_r)^{p^\mu}.p(\varepsilon_1)\ldots p(\varepsilon_{r-1})p(\varepsilon_{r+1})\cdots \equiv p(\varepsilon_r).p(\varepsilon_1)\cdots \equiv 0^{**}) \text{ (mod. } p)$$

i. e.
$$\frac{\text{Nm}\, p(\varepsilon)}{p(\varepsilon)} = \frac{p}{p(\varepsilon)} \equiv 0 \text{ (mod. } p), \text{ sive } \frac{p}{p(\varepsilon)} = p.f(\varepsilon)$$

sive denique $1 = f(\varepsilon).p(\varepsilon)$, id quod fieri non posse facile patet, si in utraque aequationis parte normam formes. Tum enim esset $1 = p.\text{Nm} f(\varepsilon)$.

§ 3.

Cum omnes numeri complexi, qui periodis constant, etiam tanquam functiones ipsarum radicum considerari possint, cumque iis quae sequuntur haec forma simplicior magis accommodata sit, hanc ipsam accipiemus, ubicunque salva quaestionum generalitate fieri poterit.

1. ***Theorema.*** Quando norma aliqua $\text{Nm} f(\omega)$ numerum primum p continet, qui ad exponentem μ modulo ν pertineat, illam ipsam normam μ^{ta} ipsius p potestas metiri debet.

Dem. Cum sit $\mu.\lambda = \nu - 1$ cumque p ad numerum μ pertineat, ponatur $p \equiv g^\lambda$. Iam erit secundum rationem saepe usitatam:

$$f(\omega) \equiv f(\omega),\ f(\omega)^p \equiv f(\omega^p),\ f(\omega)^{p^2} \equiv f(\omega^{p^2}),\ \ldots\ f(\omega)^{p^{\mu-1}} \equiv f(\omega^{p^{\mu-1}}) \text{ (mod. } p).$$

Quibus congruentiis inter se multiplicatis obtinemus:

$$f(\omega)^{1+p+p^2+\cdots+p^{\mu-1}} \equiv f(\omega).f(\omega^p)\ldots f(\omega^{p^{\mu-1}}) \text{ (mod. } p).$$

Qua in congruentia si deinceps valores: ω^g, ω^{g^2}, $\ldots$ $\omega^{g^{\lambda-1}}$ loco ipsius ω substituuntur, atque congruentiae, quae hoc modo prodeunt, inter se multiplicantur, fit:

$$\{f(\omega).f(\omega^g)\ldots f(\omega^{g^{\lambda-1}})\}^{1+p+\cdots+p^{\mu-1}} \equiv \text{Nm} f(\omega) \equiv 0 \text{ (mod. } p)$$

*) v. adnotationem secundam ad § 2.

**) v. § 3, 1.

sive posito $f(\omega).f(\omega^g)\dots f(\omega^{g^{\lambda-1}}) = \varphi(\omega)$:

$$\varphi(\omega)^{1+p+\dots+p^{\mu-1}} \equiv 0 \pmod{p}.$$

Iam cum sit $1+p+\dots+p^{\mu-1} < p^\mu$, certo etiam erit

$$\varphi(\omega)^{p^\mu} \equiv 0 \pmod{p}.$$

Est vero

$$\varphi(\omega)^{p^\mu} \equiv \varphi(\omega^{p^\mu}) \equiv \varphi(\omega) \pmod{p}, \quad \text{ergo} \quad \varphi(\omega) \equiv 0 \pmod{p},$$

unde mutatis radicibus ω oriuntur relationes:

$$\varphi(\omega) \equiv \varphi(\omega^{g^\lambda}) \equiv \varphi(\omega^{g^{2\lambda}}) \equiv \dots \equiv \varphi(\omega^{g^{(\mu-1)\lambda}}) \equiv 0 \pmod{p},$$

unde denique respecta ipsius $\varphi(\omega)$ definitione:

$$\mathrm{Nm} f(\omega) = \varphi(\omega).\varphi(\omega^{g^\lambda})\dots\varphi(\omega^{g^{(\mu-1)\lambda}}) \equiv 0 \pmod{p^\mu}.$$

2. ***Theorema.*** Normam aliquam $\mathrm{Nm} f(\omega)$ si numerus primus p metitur, qui ad exponentem μ modulo ν pertinet quique in λ factores primos complexos e periodis ε compositos dissolvi potest, quotiens illius normae et summae quae ea continetur numeri primi potestatis ipse tanquam norma repraesentari potest.

Dem. Primum adnotamus summam ipsius p potestatem numero $\mathrm{Nm} f(\omega)$ contentam secundum supra dicta multiplum ipsius μ esse debere. Iam sit $p = \mathrm{Nm}\, p(\varepsilon)$, deinde ponatur

$$f(\omega).f(\omega^{g^\lambda}).f(\omega^{g^{2\lambda}})\dots f(\omega^{g^{(\mu-1)\lambda}}) = \varphi(\varepsilon)\,^{*}).$$

Tum habemus secundum suppositionem nostram:

$$\mathrm{Nm} f(\omega) \;=\; \mathrm{Nm}\,\varphi(\varepsilon) \equiv 0 \pmod{p},$$

unde secundum § 2, 1: $\varphi(e_r) \equiv 0 \pmod{p}$ ideoque $(\mathrm{mod.}\, p(\varepsilon))$. Cumque habeamus secundum § 2, 2: $e \equiv \varepsilon \; (\mathrm{mod.}\, p(\varepsilon))$, erit: $\varphi(\varepsilon_r) \equiv 0 \; (\mathrm{mod.}\, p(\varepsilon))$, sive mutatis periodis $\varphi(\varepsilon) \equiv 0 \; (\mathrm{mod}\, p(\varepsilon_{-r}))$ i. e.

$$f(\omega).f(\omega^{g^\lambda})\dots f(\omega^{g^{(\mu-1)\lambda}}) \equiv 0 \; (\mathrm{mod.}\, p(\varepsilon_{-r})),$$

sive si congruentiam $p \equiv g^\lambda \pmod{\nu}$ respicimus:

$$f(\omega).f(\omega^p)\dots f(\omega^{p^{\mu-1}}) \equiv 0 \; (\mathrm{mod.}\, p(\varepsilon_{-r})).$$

Est vero:

$$f(\omega).f(\omega^p)\dots f(\omega^{p^{\mu-1}}) \equiv f(\omega)^{1+p+\dots+p^{\mu-1}} \pmod{p}\,^{**})$$

ideoque $(\mathrm{mod.}\, p(\varepsilon_{-r}))$, unde ratione supra exhibita colligimus esse:

$$f(\omega) \equiv 0 \; (\mathrm{mod.}\, p(\varepsilon_{-r})) \quad \text{sive} \quad f(\omega) \;=\; \psi(\omega).p(\varepsilon_{-r}).$$

---

*) *Gauss* disq. arithm. 345.

**) v. paragraphum antecedentem.

Ad normam transeuntes obtinemus aequationem:

$$\mathrm{Nm}\, f(\omega) = p^{\mu}.\mathrm{Nm}\, \psi(\omega) \quad \text{sive} \quad \mathrm{Nm}\frac{f(\omega)}{p^{\mu}} = \mathrm{Nm}\, \psi(\omega) \quad \text{q. e. d.}$$

Iam hac methodo iterum atque iterum adhibita facile patet e suppositione $\mathrm{Nm}\, f(\omega) \equiv 0 \pmod{p^{n.\mu}}$ congruentiam colligi huiusmodi:

$$f(\omega) \equiv 0 \pmod{p(\varepsilon_k)^m . p(\varepsilon_{k'})^{m'} \ldots},$$

ubi $m + m' + \cdots = n$; denique habebitur theorema hocce: quando norma aliqua divisibilis est per numerum, cuius factores primi reales in factores complexos quam plurimos discerpi possunt*), quotiens illius normae et summae quae ea continetur denominatoris potestatis ipse tanquam norma repraesentari potest.

Adnotatio. Si $\mathrm{Nm}\, f(\omega) \equiv 0 \pmod{\nu}$, habemus $f(\omega) \equiv 0 \pmod{(1-\omega)}$**), pariterque e congruentia $\mathrm{Nm}\, f(\omega) \equiv 0 \pmod{\nu^m}$ congruentiam colligimus

$$f(\omega) \equiv 0 \pmod{(1-\omega)^m}.$$

§ 4.

Sit $f(\omega)$ numerus aliquis complexus, N numerus realis eiusmodi, ut factores eius primi reales in factores complexos quam plurimos discerpi possint, sitque factor numerorum $f(\omega)$ et N communis maximus $\varphi(\omega)$***), numerus $\psi(\omega)$ inveniri potest talis, ut sit: $\psi(\omega).f(\omega) \equiv \varphi(\omega) \pmod{N}$†).

Dem. Sit primum numerus N potestas numeri primi, ergo: $N = p^{\pi}$; sit deinde $p = \mathrm{Nm}\, p(\varepsilon)$ et $p \equiv g^{\lambda} \pmod{\nu}$.

Iam erit secundum §. 3, 2:

$$f(\omega) = F(\omega).p(\varepsilon_k)^m.p(\varepsilon_{k'})^{m'} \ldots,$$

ubi $p^{m+m'+\cdots}$ summa ipsius p potestas numero $\mathrm{Nm}\, f(\omega)$ contenta. Est igitur $\mathrm{Nm}\, F(\omega)$ numerus ad ipsum p primus, quare exstat numerus x talis, ut sit: $x.\mathrm{Nm}\, F(\omega) \equiv 1 \pmod{p^{\pi}}$. Hinc habemus:

---

*) Numerum aliquem primum p ad divisorem μ ipsius $\nu - 1$ pertinentem in factores complexos quam plurimos discerpi posse dicimus, si in $\frac{\nu - 1}{\mu}$ factores complexos e periodis ε compositos eosque coniunctos dissolvi potest.

**) v. § 2, 2.

***) De factore communi maximo sermonem esse posse inde elucet, quod factores ipsius N primi in factores complexos dissolvi queunt, igitur ad eos omnes theorema § 3, 2 adhiberi potest. Caeterum hoc in ipsa demonstratione probabitur.

†) Modulum realem accipimus, quia si complexus est multiplicando per factores coniunctos realis reddi potest.

$$\text{(I.)}\quad \begin{aligned} x.F(\omega^2)\,F(\omega^3)\dots F(\omega^{\nu-1}).f(\omega) &= x.\mathrm{Nm}\,F(\omega).p(\varepsilon_k)^m.p(\varepsilon_{k'})^{m'}\dots \\ &\equiv p(\varepsilon_k)^m.p(\varepsilon_{k'})^{m'}\dots \pmod{p^\pi}. \end{aligned}$$

Designemus complexum factorum omnium et producto $p(\varepsilon_k)^m.p(\varepsilon_{k'})^{m'}\dots$ et numero p^π i. e. producto $p(\varepsilon)^\pi.p(\varepsilon_1)^\pi\dots$ communium signo $P(\varepsilon)$, ita ut sint:

$$P(\varepsilon).p(\varepsilon_a)^\alpha.p(\varepsilon_{a'})^{\alpha'}\dots = P(\varepsilon).A(\varepsilon) = p(\varepsilon_k)^m.p(\varepsilon_{k'})^{m'}\dots,$$
$$P(\varepsilon).p(\varepsilon_b)^\beta.p(\varepsilon_{b'})^{\beta'}\dots = P(\varepsilon).B(\varepsilon) = p^\pi.$$

Iam nullum indicem a nulli indici b aequalem esse patet. Sint $c, c', \dots$ indices ii, qui coniuncti cum indicibus a et b seriem $0, 1, 2, \dots \lambda-1$ efficiunt, atque posito $C(\varepsilon) = p(\varepsilon_c).p(\varepsilon_{c'})\dots$ formetur expressio:

$$V(\varepsilon) = A(\varepsilon)+B(\varepsilon).C(\varepsilon),$$

normam huius expressionis numerus p metiri nequit; tum enim pro uno valore e congruentiae $\mathrm{Nm}(e-\varepsilon)\equiv 0 \pmod{p}$ esse deberet $V(e)\equiv 0 \pmod{p}$*) i. e.

$$A(e)+B(e).C(e)\equiv 0.$$

Cum vero pro quovis e unus tantum factorum $p(e)$ nihilo congruus esse possit**), aut $A(e)$ aut $B(e)$ aut $C(e)$, minime igitur $A(e)+B(e).C(e)$, nihilo congruum erit. Quare iam existet numerus y talis, ut sit: $y.\mathrm{Nm}\,V(\varepsilon)\equiv 1 \pmod{p^\pi}$ sive substituto ipsius $V(\varepsilon)$ valore:

$$y.V(\varepsilon_1)\dots V(\varepsilon_{\lambda-1})A(\varepsilon)+y.V(\varepsilon_1)\dots V(\varepsilon_{\lambda-1})B(\varepsilon).C(\varepsilon)\equiv 1 \pmod{p^\pi}.$$

Qua congruentia in numerum $P(\varepsilon)$ ducta, atque respectu habito aequationis $B(\varepsilon).P(\varepsilon) = p^\pi$, obtinemus:

$$\text{(II.)}\quad y.V(\varepsilon_1)\dots V(\varepsilon_{\lambda-1})\,A(\varepsilon).P(\varepsilon)\equiv P(\varepsilon) \pmod{p^\pi}.$$

Unde si illam congruentiam (I):

$$x.F(\omega^2)\dots F(\omega^{\nu-1}).f(\omega)\equiv A(\varepsilon).P(\varepsilon) \pmod{p^\pi}$$

respicimus atque

$$x.F(\omega^2)\dots F(\omega^{\nu-1}).y.V(\varepsilon_1)\dots V(\varepsilon_{\lambda-1}) = \psi(\omega)$$

ponimus, denique prodit congruentia:

$$\psi(\omega).f(\omega)\equiv P(\varepsilon) \pmod{p^\pi},$$

ubi numerum $P(\varepsilon)$ factorem esse numerorum $f(\omega)$ et p^π communem maximum ex ipsa expressionis $P(\varepsilon)$ definitione elucet. Istam congruentiam si tanquam aequationem scribimus designante $G(\omega)$ numerum integrum complexum,

*) v. § 2, 1.
**) v. § 2, 4.

obtinemus:

$$\psi(\omega).f(\omega) = P(\varepsilon) + G(\omega).p^\pi \quad \text{sive} \quad \psi(\omega).\frac{f(\omega)}{p^\pi} = \frac{1}{B(\varepsilon)} + G(\omega).$$

Casu $p=\nu$ habemus $f(\omega) = (1-\omega)^\pi F(\omega)$, ubi numerus $\mathrm{Nm}\,F(\omega)$ ad ipsum ν primus est*). Iam posito $x.\mathrm{Nm}\,F(\omega) \equiv 1 \pmod{\nu^\pi}$ atque:

$$x.F(\omega^2).F(\omega^3)\ldots F(\omega^{\nu-1}) = \psi(\omega)$$

obtinemus:

$$\psi(\omega)f(\omega) \equiv (1-\omega)^\pi \pmod{\nu^\pi}.$$

Iam posito $N = p^a.q^b\ldots$, ubi $p, q, \ldots$ sunt numeri primi inter se diversi, inveniri possunt numeri $\psi(\omega)$, $\psi_2(\omega), \ldots$ tales, ut sint:

$$\psi_1(\omega).f(\omega) \equiv P(\varepsilon) \pmod{p^a}, \quad \psi_2(\omega).f(\omega) \equiv Q(\varepsilon') \pmod{q^b}, \ldots,$$

ubi $P(\varepsilon)$ factor est communis maximus numerorum $f(\omega)$ et p^a, $Q(\varepsilon')$ factor communis maximus numerorum $f(\omega)$ et q^b etc. Itaque habemus:

$$Q(\varepsilon').R(\varepsilon'')\ldots\psi_1(\omega).f(\omega) = \chi_1(\omega)f(\omega) \equiv P(\varepsilon)\,Q(\varepsilon')\ldots \pmod{p^a},$$
$$P(\varepsilon).R(\varepsilon'')\ldots\psi_2(\omega).f(\omega) = \chi_2(\omega)f(\omega) \equiv P(\varepsilon)\,Q(\varepsilon')\ldots \pmod{q^b}.$$
$$\vdots \qquad\qquad \vdots \qquad\qquad \vdots$$

Deinde numerus inveniri potest complexus $\psi(\omega)$ talis, ut sit:

$$\psi(\omega) \equiv \chi_1(\omega) \pmod{p^a}, \quad \psi(\omega) \equiv \chi_2(\omega) \pmod{q^b}, \quad \ldots,$$

quia pro singulis coefficientibus potestatum radicum ω in ipsis $\chi(\omega)$ hae ipsae congruentiae expleri possunt. Unde denique habemus:

$$\psi(\omega).f(\omega) \equiv P(\varepsilon).Q(\varepsilon').R(\varepsilon'')\ldots \pmod{N},$$

ubi dextra congruentiae pars factorem numerorum $f(\omega)$ et N communem maximum continet.

§ 5.

Dato aliquo numero primo p, qui condicionem implet $p^\mu \equiv 1 \pmod{p}$, semper exstare numerum π talem, ut sit $\pi p = \mathrm{Nm}(e-\varepsilon)$, iam supra diximus (v. §. 2). Quem numerum π generaliter ita eligere possumus, ut sit ad p primus. Quodsi enim π numerum p ideoque $\mathrm{Nm}(e-\varepsilon)$ numerum p^2 implicat, habemus:

$$\mathrm{Nm}(p+e-\varepsilon) = \pi' p = \mathrm{Nm}(e-\varepsilon) + p\{(e-\varepsilon_1)(e-\varepsilon_2)\cdots+(e-\varepsilon)(e-\varepsilon_2)\cdots+\cdots\}+p^2\{\cdots\}.$$

Iam si et ipsum π' factorem p contineret, etiam illa expressio per ipsum p

*) v. adnotationem in fine paragraphi 3.

multiplicata nihilo congrua foret modulo p. Quae expressio, tanquam functio ipsorum ε symmetrica, etiam mutatis quantitatibus ε cum numeris e nihilo congrua esse deberet. Tum autem omnes termini primo excepto evanescunt, qua de causa obtinemus:

$$(e-e_1)(e-e_2)\cdots \equiv 0 \pmod{p}$$

sive igitur

$$e \equiv e_r \pmod{p},$$

id quod fieri non potest, nisi pro certis quibusdam numeris p, qui et ipsi divisores numeri $\mathrm{Nm}(\varepsilon-\varepsilon_r)$ sunt. Quodsi enim $e \equiv e_r \pmod{p}$, est quoque:

$$(e-e_r)(e_1-e_{r+1})\ldots(e_{\lambda-1}-e_{r+\lambda-1}) \equiv 0 \equiv (\varepsilon-\varepsilon_r)(\varepsilon_1-\varepsilon_{r+1})\cdots \equiv \mathrm{Nm}(\varepsilon-\varepsilon_r) \pmod{p}.$$

Theorema. Si normam numeri complexi $\mathrm{Nm}f(\omega)$ numerus primus p metitur ad exponentem μ modulo ν pertinens atque $\pi p = \mathrm{Nm}(e-\varepsilon)$ est, numerum $\pi.f(\omega)$ aliquis factor $e-\varepsilon_k$ metiri debet.

Dem. Ponatur

$$f(\omega).f(\omega^{g^\lambda})\ldots f(\omega^{g^{(\mu-1)\lambda}}) = \varphi(\varepsilon)\text{*)}.$$

Tum habemus: $\mathrm{Nm}f(\omega) = \mathrm{Nm}\varphi(\varepsilon) \equiv 0 \pmod{p}$, ergo secundum § 2, 1:

$$\varphi(e_r) \equiv 0 \pmod{p} \text{ et } \pi.\varphi(e_r) \equiv 0 \pmod{\pi.p} \text{ ideoque } (\mathrm{mod.}\,(e-\varepsilon)).$$

Deinde cum appareat esse $e \equiv \varepsilon$ et $e_r \equiv \varepsilon_r$ $(\mathrm{mod.}\,(e-\varepsilon))$, obtinemus congruentias:

$$\pi\varphi(e_r) \equiv \pi.\varphi(\varepsilon_r) \equiv 0 \ (\mathrm{mod.}\,(e-\varepsilon)) \quad \text{sive} \quad \pi.\varphi(\varepsilon) \equiv 0 \ (\mathrm{mod.}\,(e-\varepsilon_{-r}))$$

i. e.

$$\pi.f(\omega).f(\omega^{g^\lambda})\ldots f(\omega^{g^{(\mu-1)\lambda}}) \equiv 0 \ (\mathrm{mod.}\,(e-\varepsilon_{-r}))$$

sive, si congruentiam $p \equiv g^\lambda$ respicimus,

$$\pi.f(\omega).f(\omega^p)\ldots f(\omega^{p^{\mu-1}}) \equiv 0 \ (\mathrm{mod.}\,(e-\varepsilon_{-r})).$$

Est vero

$$\pi.f(\omega).f(\omega^p)\ldots f(\omega^{p^{\mu-1}}) \equiv \pi.f(\omega)^{1+p+\ldots+p^{\mu-1}} \pmod{\pi p} \text{ ideoque } (\mathrm{mod.}\,(e-\varepsilon_{-r}))$$

ergo ratione supra adhibita:

$$\pi.f(\omega) \equiv 0 \ (\mathrm{mod.}\,(e-\varepsilon_{-r})) \quad \text{q. e. d.}$$

Qua ratione iterata facile supposita congruentia $\mathrm{Nm}f(\omega) \equiv 0 \pmod{p^{n.\mu}}$ colligimus congruentiam locum habere huiusmodi:

$$\pi^n.f(\omega) \equiv 0 \ (\mathrm{mod.}\,(e-\varepsilon_k)^m.(e-\varepsilon_{k'})^{m'}\ldots),$$

ubi $m+m'+\cdots = n$ est.

---

*) v. *Gauss* disq. arithm. 345.

§ 6.

Sit p numerus primus talis, ut sit $p^\mu \equiv 1 \pmod{\nu}$ atque $\pi p = \mathrm{Nm}(e-\varepsilon)$, sitque π numerus ad ipsum p primus. Deinde ponatur

$$(e-\varepsilon_1)(e-\varepsilon_2)\dots(e-\varepsilon_{\lambda-1}) = \varphi(\varepsilon),$$

ubi $\varphi(\varepsilon)$ ipsum p metiri non posse patet, quia posito $\varphi(\varepsilon) = p.\psi(\varepsilon)$ esset

$$(e-\varepsilon).\varphi(\varepsilon) = \mathrm{Nm}(e-\varepsilon) = \pi p = p.(e-\varepsilon)\psi(\varepsilon),$$

ergo

$$\pi = (e-\varepsilon)\psi(\varepsilon) \text{ et } \pi^\lambda = \pi p.\mathrm{Nm}\psi(\varepsilon),$$

unde sequeretur, ut ipsum π per numerum p divisibile esset. — Iam numero complexo fracto $\frac{p}{\varphi(\varepsilon)}$ tanquam modulo ad hanc quae sequitur disquisitionem utamur; id quod facile fieri potest, si statuamus

congruentiam $a \equiv b \left(\mathrm{mod.}\ \frac{m}{n}\right)$ locum tenere huiusce $an \equiv bn \pmod{m}$.

Iam patet esse

$$e \equiv \varepsilon \left(\mathrm{mod.}\ \frac{p}{\varphi(\varepsilon)}\right);$$

est enim re vera

$$(e-\varepsilon)\varphi(\varepsilon) \equiv 0 \pmod{p}, \quad \text{quia} \quad (e-\varepsilon)\varphi(\varepsilon) = \mathrm{Nm}(e-\varepsilon) = \pi p.$$

Deinde si numerus complexus $f(\varepsilon)$ congruentiae sufficit

$$f(\varepsilon) \equiv 0 \left(\mathrm{mod.}\ \frac{p}{\varphi(\varepsilon)}\right),$$

numerus p eius normam metiatur oportet. Ex ista enim congruentia concluditur $f(\varepsilon).\varphi(\varepsilon) \equiv 0 \pmod{p}$ sive $\mathrm{Nm}f(\varepsilon).\mathrm{Nm}\varphi(\varepsilon) \equiv 0 \pmod{p^\lambda}$, et cum habeamus $\mathrm{Nm}\varphi(\varepsilon) = p^{\lambda-1}\pi^{\lambda-1}$, obtinemus $\pi^{\lambda-1}\mathrm{Nm}f(\varepsilon) \equiv 0 \pmod{p}$, et quia π ad ipsum p primus est,

$$\mathrm{Nm}f(\varepsilon) \equiv 0 \pmod{p}.$$

Ex illa congruentia

$$e \equiv \varepsilon \left(\mathrm{mod.}\ \frac{p}{\varphi(\varepsilon)}\right)$$

sequitur, ut quivis numerus complexus numero reali congruus sit, scilicet

$$f(\varepsilon) \equiv f(e) \left(\mathrm{mod.}\ \frac{p}{\varphi(\varepsilon)}\right),$$

unde p residua hoc modulo incongrua exstare elucet eaque numeri $0, 1, 2, \dots p-1$. Etenim plures non existere inde patet, quod quivis numerus complexus numero

reali quivis autem numerus realis uni illorum numerorum modulo p, etiamque igitur modulo $\frac{p}{\varphi(\varepsilon)}$, congruus est. Sin vero duo illorum numerorum inter se congrui essent, earum differentia nihilo congrua fieret. Quam si litera d designamus, esset $d.\varphi(\varepsilon) \equiv 0 \pmod{p}$, ergo $d^\lambda.\mathrm{Nm}\,\varphi(\varepsilon) = d^\lambda.\pi^{\lambda-1}.p^{\lambda-1} \equiv 0 \pmod{p^\lambda}$, ergo: $d^\lambda.\pi^{\lambda-1} \equiv 0 \pmod{p}$, id quod esse nequit, quia π ad ipsum p primus atque $d < p$ est.

Iam accepto numero k eiusmodi, ut sit $k^\lambda \leqq p < (k+1)^\lambda$, statuamus cunctos numeros complexos formae $c + c_1\varepsilon + \cdots + c_{\lambda-1}\varepsilon^{\lambda-1}$, in quibus coefficientes isti c valores $0, 1, 2, \ldots k$ induunt. Horum multitudo erit $(k+1)^\lambda > p$, inter quos igitur certe duo inter se congrui erunt secundum modulum $\frac{p}{\varphi(\varepsilon)}$. Quorum altero ab altero subtracto obtinemus numerum complexum $f(\varepsilon)$, cuius coefficientes omnes inter $-k$ et $+k$ sunt, et cuius norma numerum p continet, cum ipse nihilo congruus sit modulo $\frac{p}{\varphi(\varepsilon)}$. Quare sit $\mathrm{Nm}\,f(\varepsilon) = np$. Iam si litera M_λ maximum valorem expressionis

$$\mathrm{Nm}(x + x_1\varepsilon + \cdots + x_{\lambda-1}\varepsilon^{\lambda-1})$$

designamus, ea condicione ut quantitates x cunctae inter -1 et $+1$ sint, obtinemus:

$$\frac{np}{k^\lambda} = \mathrm{Nm}\frac{f(\varepsilon)}{k}, \quad \text{ideoque} \quad \frac{np}{k^\lambda} < M_\lambda$$

sive

$$np < M_\lambda k^\lambda < M_\lambda p, \quad \text{unde denique} \quad n < M_\lambda.$$

Hinc habemus hoc theorema magni momenti. Dato aliquo numero p, qui condicionem implet $p^\mu \equiv 1 \pmod{\nu}$, semper invenire licet numerum n minorem finita quadam quantitate ab ipso p independente eumque talem, ut productum np in λ factores complexos coniunctos dissolvi possit. Quod theorema respondet illi in theoria formarum quadraticarum theoremati fundamentali, secundum quod numerus formarum reductarum finitus est. Etiam adnotandum illam rationem agendi adhiberi non posse ad eos numeros primos p, qui divisores sunt numerorum $\mathrm{Nm}(\varepsilon - \varepsilon_r)$, quarum igitur multitudo finita est. — Deinde ope huius theorematis, quantitate M determinata, numerus quam minimus inveniri potest numerorum n, quibus opus est, ut pro quolibet numero primo p, proprietate supra dicta praedito, unum productorum np norma numeri complexi sit.

Ut pro certis quibusdam numeris ν pro quovis ipsius $\nu-1$ divisore λ omnes numeri primi, residua λ^{tarum} potestatum ipsius ν, in λ factores com-

plexos dissolvi possint *), tantummodo necesse est, numeros primos, qui sint residua λ^{tae} potestatis modulo ν quantitatibus illis M_λ minores, in λ factores complexos coniunctos discerpi posse **). — Sit enim λ divisor ipsius $\nu-1$, designetur deinde signo d quilibet ipsius λ divisor excepto ipso λ; probandum est, quemvis numerum primum, residuum λ^{tae} potestatis, in λ factores complexos dissolvi posse, simodo hoc pro numeris primis p ipso M_λ minoribus eveniat praetereaque omnes numeri primi, residua d^{tarum} potestatum, in d factores complexos discerpi possint. Cum enim np tanquam norma repraesentari liceat, cumque factores ipsius n primi aut residua d^{tarum} potestatum aut residua λ^{tae} potestatis iique $\leqq n < M_\lambda$ sint ideoque in factores complexos discerpi possint, respectu habito theorematis § 3, 2 sententiam illam probari elucet. Iam primum pro ipso λ factores ipsius $\nu-1$ primos accipientes, illa quae ad divisores numeri λ spectat condicione sublata, ea tantum restat, ut numeri primi, residua λ^{tae} potestatis quantitate M_λ minores, in λ factores complexos discerpi possint. Deinde transeundo ad eos ipsius λ divisores, qui duabus tantum numeris primis constant, similem condicionem adiiciendam tantum esse patet; eaque ipsa ratione ad divisores ipsius $\nu-1$, e pluribus factoribus primis compositos, progredientes denique illam condicionem supra indicatam obtineri liquet. — Ita, ut unum tantum exemplum afferamus, posito $\nu = 5$ pro ipso numero $\nu-1 = 4$ simplicissimis iam adiumentis $M_4 = 49$ invenitur. Iam vero tres numeri primi formae $5n+1$ ipso M minores, scilicet 11, 31, 41, in quatuor factores complexos coniunctos, e radicibus unitatis quintis compositos, discerpi possunt***). Deinde pro divisore $\lambda = 2$ omnes numeri primi, residua ipsius 5 quadratica, in duos factores complexos $(a+a_1\varepsilon).(a+a_1\varepsilon_1)$ dissolvi possunt. Id quod vel illa ipsa ratione erui vel e theoria formarum secundi gradus probari potest. Est enim

$$(a+a_1\varepsilon)(a+a_1\varepsilon_1) = (a+a_1\omega+a_1\omega^{-1}).(a+a_1\omega^2+a_1\omega^{-2}) = a^2-aa_1-a_1^2.$$

Hinc igitur quemvis numerum primum formae $5n+1$ in quatuor, quemvis numerum primum formae $5n-1$ in duos factores complexos coniunctos, e radicibus unitatis quintis compositos, discerpi posse colligimus.

*) Adnotamus illud etiam ita exhiberi posse, ut pro his numeris ν omnes numeros primos formarum $k\nu+g^\lambda$ in λ factores complexos coniunctos dissolvi posse dicamus. Id quod illi sententiae aequivalere e facili consideratione elucet.

**) Addendum est praeterea eos numeros primos, qui numeros $\mathrm{Nm}(\varepsilon-\varepsilon_r)$ metiantur, pro se quosque disquirendos esse.

***) v. Cli. *Kummer* disput. pag. 21.

§ 7.

Iam transeuntes ad numeros ν compositos adnotamus, nos plerumque, ut iteratione supersedere possimus, ad methodos pro numeris primis exhibitas lectorem delegaturos esse, quippe quae in his quae sequantur paucis exceptis prorsus adhiberi possint.

Ponatur numerus compositus $\nu = a^{\alpha}.b^{\beta}.c^{\gamma}\ldots$ designantibus $a, b, c, \ldots$ numeros primos inter se diversos, sitque ω radix primitiva aequationis $x^{\nu} = 1$; hanc ipsam radicem esse aequationis:

$$f(x) = \frac{(x^{\nu}-1)(x^{\frac{\nu}{ab}}-1)(x^{\frac{\nu}{ac}}-1)\ldots}{(x^{\frac{\nu}{a}}-1)(x^{\frac{\nu}{b}}-1)(x^{\frac{\nu}{c}}-1)\ldots} = 0$$

notis methodis probatur, quae quidem aequatio $\varphi(\nu)^{\text{ti}}$ gradus*) omnes ν^{tas} radices unitatis primitivas amplectitur. Hanc vero aequationem reduci non posse, sive radices quasdam ω aequatione inferioris gradus atque coefficientium integrorum contineri non posse, hic probare omittimus**), cum limites huius libelli demonstrationem hic tradere non patiantur. Ex ea vero aequationis illius proprietate sequitur, ut quaecunque functio ipsius ω integra pro quibusdam ipsius ω valoribus evanescat eadem pro omnibus quoque reliquis valoribus nihilo aequalis fiat. Quod nisi fieret, factor communis maximus istius functionis et functionis $f(x)$, cum et idem functio sit integra, tamen illas certas tantum radices ω haberet atque factor functionis $f(x)$ foret, id quod fieri nequit. — Iam designentur radices primitivae numerorum $a^{\alpha}, b^{\beta}, \ldots$ resp. literis $g, h, \ldots$, deinde ponatur $\frac{\nu}{a^{\alpha}} = a'$, $\frac{\nu}{b^{\beta}} = b'$, $\ldots$; tum forma

$$a'g^{m} + b'h^{n} + \cdots$$

systema numerorum ad numerum ν primorum atque inter se incongruorum contineri constat, si numeris $m, n, \ldots$ sensim sensimque resp. valores $1, 2, \ldots a^{\alpha-1}(a-1)$; $1, 2, \ldots b^{\beta-1}(b-1)$; etc. tribuuntur. — Nunc sit λ divisor aliquis ipsius $a^{\alpha-1}(a-1)$ talis, ut multiplum sit ipsius $a^{\alpha-1}$, λ' divisor ipsius $b^{\beta-1}(b-1)$, multiplum ipsius $b^{\beta-1}$, etc., ita ut habeamus

$$\lambda\mu = a^{\alpha-1}(a-1), \quad \lambda'\mu' = b^{\beta-1}(b-1), \quad \ldots,$$

*) $\varphi(\nu)$ numerus ille est numerorum ad ipsum ν primorum eoque minorum.

**) Demonstrationem illam, de qua sermo est, proximo tempore in publicum editurus sum.

et ponatur:

$$\varepsilon_{k,k',\ldots} = \sum_{m=0}^{m=\mu-1} \sum_{n=0}^{n=\mu'-1} \ldots \omega^{a'g^{m\lambda+k}+b'h^{n\lambda'+k'}+\cdots}$$

sive

$$\varepsilon_{k,k',\ldots} = \sum_m \omega^{a'g^{m\lambda+k}} . \sum_n \omega^{b'h^{n\lambda'+k'}} \ldots,$$

quae expressiones partes periodorum in numeris primis ν agunt. — Numerus terminorum expressionis talis erit: $\mu.\mu'.\mu''\ldots$, numerus periodorum ε inter se diversarum: $\lambda.\lambda'.\lambda''\ldots$, cum quantitates $k, k', \ldots$ resp. valores $0, 1, 2, \ldots \lambda-1$; $0, 1, 2, \ldots \lambda'-1$; etc. induere possint.

Productum $\Pi(x-\varepsilon)$, ubi signum Π in omnes ipsius ε valores extendi debet, functionem radicum ω symmetricam ideoque integris potestatum x coefficientibus gaudere apparet. — Per aequationem $\Pi(x-\varepsilon)=0$, quippe quae sit gradus $\lambda.\lambda'.\lambda''\ldots$, quaevis ipsius ε potestas $\geqq \lambda\lambda'\lambda''\ldots$ potestatibus inferioribus exprimi potest.

Duae periodi ε diversorum indicum aequales esse non possunt.

Primum enim ex aequatione $\varepsilon_{0,0,\ldots} = \varepsilon_{k,k',k'',\ldots}$ sequeretur aequatio eiusmodi $\varepsilon_{0,0,\ldots} = \varepsilon_{k,mk',nk'',\ldots}$ *) designantibus $m, n, \ldots$ numeros quoscunque integros. Iam ponendo $m = b^{\beta-1}(b-1)$, $n = c^{\gamma-1}(c-1)$, etc. obtinemus $\varepsilon_{0,0,0,\ldots} = \varepsilon_{k,0,0,\ldots}$ sive respecta illa altera ipsorum ε definitione atque sublatis factoribus utriusque partis communibus:

$$\Sigma\omega^{a'g^{m\lambda}} = \Sigma\omega^{a'g^{m\lambda+k}},$$

cumque $\omega^{a'}$ sit radix aequationis $x^{a^\alpha}=1$ primitiva, pro iis unitatis radicibus, quae ad numerorum primorum potestates pertinent, illud theorema demonstrare sufficit. Quem ad finem designamus brevitatis causa signo ε_k expressionem $\Sigma\omega^{a'g^{m\lambda+k}}$ et ipsam radicem unitatis $a^{\alpha\text{tam}}$ primitivam litera ω, ponatur denique $a^{\alpha-1}(a-1) = \mathfrak{a}$, ita ut habeamus $\varepsilon_k = \Sigma\omega^{g^{m\lambda+k}}$. Iam colliguntur ex aequatione $\varepsilon_0 = \varepsilon_k$ haece: $\varepsilon_1 = \varepsilon_{k+1}$, $\varepsilon_2 = \varepsilon_{k+2}$, etc., unde igitur:

$$\text{I.} \quad \varepsilon + \varrho\varepsilon_1 + \varrho^2\varepsilon_2 + \cdots + \varrho^{\lambda-1}\varepsilon_{\lambda-1} = \varepsilon_k + \varrho\varepsilon_{k+1} + \varrho^2\varepsilon_{k+2} + \cdots + \varrho^{\lambda-1}\varepsilon_{k+\lambda-1},$$

ubi ϱ radix quaecunque sit aequationis $x^{\mathfrak{a}} = 1$. Posito:

$$\omega + \varrho\omega^g + \varrho^2\omega^{g^2} + \cdots + \varrho^{\mathfrak{a}-1}\omega^{g^{\mathfrak{a}-1}} = (\varrho, \omega)$$

obtinemus secundum I pro quovis ipsius ϱ valore, qui radix est aequationis $x^\lambda = 1$:

$$(\varrho, \omega) = (\varrho, \omega^{g^k}) = (\varrho, \omega).\varrho^{-k}, \text{ unde } (\varrho, \omega)\,(1-\varrho^{-k}) = 0,$$

---

*) Nempe mutando ipsum ω, id quod secundum supra dicta facere licet.

id quod certe fieri non posse pro radicibus ϱ aequationis $x^\lambda = 1$ primitivis iam probemus. Pro his enim $1-\varrho^{-k}$ evanescere nequit, quia $k < \lambda$ est. Deinde (ϱ, ω) non evanescit, quod demonstrari potest*) productum $(\varrho, \omega)(\varrho^{-1}, \omega) = \pm a^a$ evadere nisi $\varrho^{a^{\alpha-2}(a-1)} = 1$; cumque λ multiplum ipsius $a^{\alpha-1}$ atque ϱ radicem aequationis $x^\lambda = 1$ primitivam supposuerimus, radicem ϱ aequationi $\varrho^{a^{\alpha-2}(a-1)} = 1$ sufficere non posse ideoque quantitatem (ϱ, ω) non evanescere facile perspicitur.

Posito A, A_1, ... numeros reales integros esse, expressio formae:

$$A + A_1\varepsilon + A_2\varepsilon^2 + \cdots + A_{L-1}\varepsilon^{L-1} = f(\varepsilon)^{**})$$

numerus complexus dicetur.

Ex aequatione $f(\varepsilon) = 0$ colligitur $f(\varepsilon_k) = 0$, quia $f(\varepsilon)$ radicum ω functio est integra. — Deinde e relatione $f(\varepsilon) = 0$ colligimus esse $A = A_1 = A_2 = \cdots = 0$. Cum enim $f(x)$ pro omnibus periodis ε i. e. pro L valoribus ipsius x (quos inter se diversos esse supra probavimus) evanescat, tamenque gradus tantum $L-1^{ti}$ sit, coefficientes evanescere necesse est. Unde haec theoremata patent: duabus numeris complexis inter se aequalibus et singuli numeri coniuncti et coefficientes resp. aequales sunt.

Quaevis periodus $\varepsilon_{k,k',k'',\ldots}$ tanquam functio integra coefficientium rationalium unius periodi repraesentari potest. Ad quod probandum primum numerus ν potestas numeri primi ($\nu = a^\alpha$) ponendus est. Iam designante litera ω radicem primitivam aequationis $x^{a^\alpha} = 1$ ponatur:

$$\omega^{g^k} + \omega^{g^{\lambda+k}} + \cdots + \omega^{g^{(\mu-1)\lambda+k}} = \varepsilon_k = \varepsilon(\omega^{g^k}),$$

denique $\lambda = a^{\alpha-1}.d$ et $d.\mu = a-1$. — Radix ω cum aequationi sufficiat:

$$1 + \omega^{a^{\alpha-1}} + \omega^{2a^{\alpha-1}} + \cdots + \omega^{(a-1)a^{\alpha-1}} = 0$$

ideoque

$$\omega^r + \omega^{r+a^{\alpha-1}} + \omega^{r+2a^{\alpha-1}} + \cdots + \omega^{r+(a-1)a^{\alpha-1}} = 0,$$

habemus aequationes:

$$\varepsilon(\omega^r) + \varepsilon(\omega^{a^{\alpha-1}+r}) + \cdots + \varepsilon(\omega^{(a-1)a^{\alpha-1}+r}) = 0,$$

in quibus numerus r valores 1, 2, ... $a^{\alpha-1}-1$ induere potest. Inter quas vero quaeque μ inter se congruunt, unde numerus aequationum inter se di-

*) Id quod fusius exponere omittimus.
**) Posuimus $L = \lambda.\lambda'.\lambda''\ldots$

versarum est $\frac{a^{\alpha-1}-1}{\mu}+1$, addita illa aequatione pro $r=0$ scilicet:

$$\mu+\varepsilon(\omega^{a^{\alpha-1}})+\cdots+\varepsilon(\omega^{(a-1)a^{\alpha-1}})=0.$$

Numerus expressionum omnium $\varepsilon(\omega^r)$ inter se diversarum est $\frac{a^\alpha-1}{\mu}$, quarum autem $\frac{a^{\alpha-1}-1}{\mu}+1$ reliquis per illas aequationes lineariter exprimere licet; qua de causa tantum $\frac{a^\alpha-a^{\alpha-1}}{\mu}-1$ sive $\lambda-1$ restant. Iam quamvis ipsius $\varepsilon(\omega^{g^k})$ potestatem tanquam functionem linearem *omnium* expressionum $\varepsilon(\omega^r)$ ideoque tanquam functionem linearem aliquarum $(\lambda-1)$ quantitatum $\varepsilon(\omega^r)$ repraesentari posse nullo negotio perspicitur. Qua de causa ponamus potestates $\varepsilon_k^2, \varepsilon_k^3, \ldots \varepsilon_k^{\lambda-1}$ repraesentatas $\lambda-1$ expressionibus $\varepsilon(\omega^r)$, inter quas sint ε_k et $\varepsilon(\omega^n)$. Ex quibus $\lambda-2$ aequationibus, reliquis $\lambda-3$ quantitatibus $\varepsilon(\omega^r)$ eliminatis, restabit aequatio huius formae:

$$A+A_1\varepsilon_k+A_2\varepsilon_k^2+\cdots+A_{\lambda-1}\varepsilon_k^{\lambda-1}=B\varepsilon(\omega^n),$$

ubi certe non omnes coefficientes A evanescere possunt. Coefficientem B evanescere non posse, solutionem igitur non illusoriam esse, inde elucet, quod functio periodi ε_k gradus $(\lambda-1)^{ti}$ integra evanescere nequit, nisi ipsi coefficientes nihilo aequales sunt*).

Quodsi iam ν numerum aliquem compositum ponimus, atque

$$\Sigma\omega^{a'g^{m\lambda+k}}=\varepsilon_k,\quad \Sigma\omega^{b'h^{n\lambda+k'}}=\varepsilon'_{k'},\ \text{etc.}$$

igitur secundum illam definitionem: $\varepsilon_{k,k',\ldots}=\varepsilon_k.\varepsilon'_{k'}\ldots$ scimus hoc productum exprimi posse producto functionum rationalium ipsorum $\varepsilon, \varepsilon', \varepsilon'', \ldots$. Restat igitur, ut probemus quodvis productum $\varepsilon^i.\varepsilon'^{i'}\ldots$ repraesentari posse potestatibus $(\varepsilon.\varepsilon'.\varepsilon''\ldots)$, $(\varepsilon.\varepsilon'.\varepsilon''\ldots)^2$, $\ldots$ $(\varepsilon.\varepsilon'.\varepsilon''\ldots)^{L-1}$. Cum vero quaeque i^{ta} ipsius ε potestas potestate prima, secunda, etc., $(\lambda-1)^{ta}$ exprimi possit, illae $L-1$ potestates quantitatis $(\varepsilon.\varepsilon'.\varepsilon''\ldots)$ repraesentari possunt variis productis $\varepsilon^i.\varepsilon'^{i'}\ldots$, in quibus $i<\lambda$, $i'<\lambda'$, $\ldots$, quorum igitur numerus est $\lambda.\lambda'.\lambda''\ldots=L$, vel excepto producto $\varepsilon^0.\varepsilon'^0\cdots=1$ restant $L-1$ producta, quibus potestates $(\varepsilon.\varepsilon'\ldots)^2$, $(\varepsilon.\varepsilon'\ldots)^3$, ... expressae sunt. Ex quibus aequationibus $L-2$ si omnia eliminamus producta exceptis $\varepsilon.\varepsilon'.\varepsilon''\ldots$ et certo quodam $\varepsilon^i.\varepsilon'^{i'}\ldots$, quorum igitur multitudo $L-3$, obtinemus aequationem formae:

$$A+A_1(\varepsilon.\varepsilon'\ldots)+A_2(\varepsilon.\varepsilon'\ldots)^2+\cdots+A_{L-1}(\varepsilon.\varepsilon'\ldots)^{L-1}=B\varepsilon^i.\varepsilon'^{i'}\ldots,$$

*) Id quod ratione supra (pag. 19) exhibita probatur.

in qua certe non omnes coefficientes A evanescere possunt. Ideoque coefficientem B non evanescere inde patet, quod functio periodi ε gradus $L-1^{\text{ti}}$ evanescere nequit, nisi omnes eius coefficientes evanescunt (v. supra pag. 19).

Ex quibus dictis satis elucet, quodque numerorum complexorum productum rursus in formam:

$$A+A_1\varepsilon+A_2\varepsilon^2+\cdots+A_{L-1}\varepsilon^{L-1}$$

redigi posse ideoque et ipsum numerum complexum esse.

Productum numerorum coniunctorum omnium norma appellatur et sicut supra signo $\mathrm{Nm}\, f(\varepsilon)$ denotatur.

Iam eadem ratione, qua Cl. *Kummer* in numeris primis ν demonstravit congruentiam λ^{ti} gradus $\mathrm{Nm}(x-\varepsilon)\equiv 0 \pmod{p}$ habere λ radices, et numero primo p sufficiente condicioni $p^{\mu}\equiv 1 \pmod{\nu}$ et casu $p=\nu$ (v. § 2), id quod huic rei respondet, posito ν numerum esse compositum, probari potest: scilicet congruentiam gradus $\lambda\lambda'\lambda''\ldots$ hanc $\mathrm{Nm}(x-\varepsilon)\equiv 0 \pmod{p}$ habere totidem radices reales, si p supponitur numerus talis, ut sit $p^{\mu}\equiv 1 \pmod{a^{\alpha}}$, $p^{\mu'}\equiv 1 \pmod{b^{\beta}}$, ..., vel etiam pro aliquo ipso ipsius ν factore primo e. g. $p=a$, dummodo $a^{\mu'}\equiv 1 \pmod{b^{\beta}}$ etc. sit*).

Pro talibus numeris primis p, quales tantum congruentiis sufficiunt

$$p^{a^k.\delta}\equiv 1 \pmod{a^{\alpha}},\quad p^{b^{k'}.\delta'}\equiv 1 \pmod{b^{\beta}},\quad \ldots,$$

ubi δ, δ'... divisores numerorum $a-1$, $b-1$, ..., numeri autem k, k', ... vel omnes vel partim >0 sunt, erit $\mathrm{Nm}(x-\varepsilon)\equiv 0 \pmod{p}$ designante ε periodum compositam e radicibus primitivis aequationis $z^{a^{\alpha-k}b^{\beta-k'}\cdots}=1$ atque habebuntur $\dfrac{\varphi(\nu)}{a^k.\delta.b^{k'}.\delta'\ldots}$ istius congruentiae radices x.

Quibus iam praeparatis theoremata iis, quae in paragraphis 2—6 pro numeris primis ν tradita sunt, respondentia nullo fere negotio pro numeris compositis ν probari possunt.

---

*) Id quod etiam e theoremate quodam generali a Clo. *Schoenemann* tradito colligi potest (*Crelles* Journal Bd. 19, S. 293).

PARS ALTERA.

§ 8.

Posito literas ν, μ, λ, ω, ε eandem habere vim quam in § 1 etiamque acceptis numeris complexis formae illius:

$$a\varepsilon + a_1\varepsilon_1 + \cdots + a_{\lambda-1}\varepsilon_{\lambda-1} = f(\varepsilon)$$

numerum talem complexum, cuius norma sit ± 1, unitatem complexam vocamus.

Disquisitio igitur unitatum complexarum eadem est, quae disquisitio formarum quarundam altiorum graduum $F = 1$. Normam enim numeri

$$a\varepsilon + a_1\varepsilon_1 + \cdots + a_{\lambda-1}\varepsilon_{\lambda-1}$$

formam esse λ^{ti} gradus atque λ indeterminatarum a, a_1, ... $a_{\lambda-1}$ et quidem determinantis, ut ita dicam, numeri primi ν sponte patet*). Quas aequationes $F = 1$ fere partes aequationis Pellianae agere imprimis ex eo elucet, quod casu $\lambda = 2$ atque $\nu \equiv 1$ (mod. 4) fit

$$\varepsilon = -\tfrac{1}{2} + \tfrac{1}{2}\sqrt{\nu}, \quad \varepsilon_1 = -\tfrac{1}{2} - \tfrac{1}{2}\sqrt{\nu},$$

unde:

$$\text{Nm} f(\varepsilon) = \tfrac{1}{4}\{(a+a_1)^2 - \nu(a-a_1)^2\}.$$

Nunc primum adnotamus ipsas unitatis radices ω unitates simplices appellari atque quamlibet unitatem complexam, unitate simplici multiplicatam, realem reddi posse demonstrabimus, in qua demonstratione Cli. *Kummer* vestigia fere omnino sequemur**).

Cum omnis periodorum functio etiam tanquam ipsarum radicum functio considerari possit, ponimus $f(\varepsilon) = \varphi(\omega)$, sitque $\text{Nm} f(\varepsilon) = 1$, ergo etiam $\text{Nm}\,\varphi(\omega) = 1$. Sit porro

$$\frac{\varphi(\omega)}{\varphi(\omega^{-1})} = \psi(\omega),$$

quem numerum integrum esse apertum est, scilicet

$$\psi(\omega) = \varphi(\omega)^2 \varphi(\omega^2) \ldots \varphi(\omega^{\nu-2}).$$

Iam posito

$$\psi(\omega) = c + c_1\omega + c_2\omega^2 + \cdots + c_{\nu-1}\omega^{\nu-1}$$

*) Cf. *Eisenstein* „de formis cubicis etc." (*Crelles* Journal, Bd. 28).

**) Disputatio Cli. *Kummer* § 4.

additis aequationibus:

$$\psi(\omega).\psi(\omega^{-1}) = 1, \quad \psi(\omega^2).\psi(\omega^{-2}) = 1, \quad \ldots \quad \psi(\omega^{\nu-1}).\psi(\omega^{-(\nu-1)}) = 1$$

obtinemus:

$$\nu(c^2+c_1^2+\cdots+c_{\nu-1}^2)-(c+c_1+\cdots+c_{\nu-1})^2 = \nu-1 \text{*)},$$

unde

$$c+c_1+\cdots+c_{\nu-1} \equiv \pm 1 \pmod{\nu},$$

quocirca haec coefficientium summa etiam aequalis ± 1 accipi potest. Itaque habemus:

$$c^2+c_1^2+\cdots+c_{\nu-1}^2 = 1,$$

unde sequitur, ut esse debeat $c_n = \pm 1$, omnes reliqui vero numeri c nihilo aequales. Invenimus igitur

$$\psi(\omega) = \frac{\varphi(\omega)}{\varphi(\omega^{-1})} = \pm\omega^n$$

esse, unde (cum signum $+$ valere ex congruentia $\varphi(\omega) \equiv \omega^n \varphi(\omega^{-1}) \pmod{(1-\omega)}$ colligere possimus):

$$\varphi(\omega) = \omega^n.\varphi(\omega^{-1})$$

atque posito $-n \equiv 2m \pmod{\nu}$ denique:

$$\omega^m\varphi(\omega) = \omega^{-m}\varphi(\omega^{-1}).$$

Ex qua aequatione apparet, quamlibet unitatem $\varphi(\omega)$, multiplicando per unitatem quandam simplicem, talem fieri posse, ut mutato ω in ω^{-1} immutata maneat, i. e. ut functio ipsorum $\omega+\omega^{-1}$, $\omega^2+\omega^{-2}$, ..., ergo realis evadat. Igitur si ad unitates formae $f(\varepsilon)$ revertimur, unitates complexae tanquam functiones periodorum *paris* terminorum numeri accipi possunt.

Iam ostendemus pro quibusvis numeris ν et λ unitates existere infinite multas easque inter se diversas. Posito enim:

$$\varphi(\omega) = \frac{(1-\omega^g)(1-\omega^{g^{\lambda+1}})\ldots(1-\omega^{g^{(\mu-1)\lambda+1}})}{(1-\omega)(1-\omega^{g^\lambda})\ldots(1-\omega^{g^{(\mu-1)\lambda}})} = \psi(\varepsilon)$$

normam huius expressionis unitati aequalem facile patet, cum norma et numeratoris et denominatoris sit ν^μ. Deinde illam expressionem numerum complexum integrum esse patet, cum pro se quisque factor numeratoris $(1-\omega^{g^{k\lambda+1}})$ factore quodam denominatoris $(1-\omega^{g^{k\lambda}})$ dividi possit, quia $\frac{1-\omega^{g^{k\lambda+1}}}{1-\omega^{g^{k\lambda}}} = \frac{1-x^g}{1-x}$ posito $\omega^{g^{k\lambda}} = x$. Denique illa expressio functio periodorum ε est, quia mu-

*) Cf. id quod pag. 4 exposuimus.

tata radice ω in $\omega^{g^{k\lambda}}$ immutata manet. Hinc igitur patet $\psi(\varepsilon)$ unitatem esse integram complexam. — Etiamque producta:

$$\psi(\varepsilon)^{n}.\psi(\varepsilon_1)^{n_1}\dots\psi(\varepsilon_{\lambda-1})^{n_{\lambda-1}},$$

designantibus $n_1, n_2, \dots n_{\lambda-1}$ quoscunque numeros integros, unitates integras complexas esse apparet, quas quidem omnes inter se diversas infra probabimus.

Adnotamus quamvis quantitatem $\psi(\varepsilon_k)$ positivam realem esse. Etenim cum numerus μ par suppositus sit, cuique factori

$$1-\omega^{g^{n\lambda+k+1}} \quad \text{factor} \quad 1-\omega^{-g^{n\lambda+k+1}}$$

respondet. Quibus multiplicatis obtinemus $2-2\cos v = 4\sin^2\frac{1}{2}v$, ubi

$$v = \frac{2}{\nu}.g^{n\lambda+k+1}.\pi.$$

Unde iam et numeratorem et denominatorem ipsius $\psi(\varepsilon_k)$ positivum esse elucet.

§ 9.

Sit unitas illa $\psi(\varepsilon) = c\varepsilon + c_1\varepsilon_1 + \dots + c_{\lambda-1}\varepsilon_{\lambda-1}$, quam positivam realem esse modo demonstravimus, atque ponatur:

$$\text{(I.)} \quad \begin{cases} c\varepsilon \quad + c_1\varepsilon_1 + \dots + c_{\lambda-1}\varepsilon_{\lambda-1} = r_1, \\ c\varepsilon_1 \quad + c_1\varepsilon_2 + \dots + c_{\lambda-1}\varepsilon \quad = r_2, \\ \quad \vdots \qquad \vdots \qquad \vdots \\ c\varepsilon_{\lambda-1} + c_1\varepsilon \quad + \dots + c_{\lambda-1}\varepsilon_{\lambda-2} = r_\lambda. \end{cases}$$

Deinde sit data aliqua unitas $a\varepsilon + a_1\varepsilon_1 + \dots + a_{\lambda-1}\varepsilon_{\lambda-1}$ atque designentur similiter valores absoluti factorum coniunctorum resp. literis $f_1, f_2, \dots f_\lambda$. Iam ponantur:

$$\text{(II.)} \quad \begin{cases} f_1 \quad = r_1^{n_1} \;.r_2^{n_2}\dots r_{\lambda-1}^{n_{\lambda-1}}, \\ f_2 \quad = r_2^{n_1} \;.r_3^{n_2}\dots r_\lambda^{n_{\lambda-1}}, \\ f_3 \quad = r_3^{n_1} \;.r_4^{n_2}\dots r_1^{n_{\lambda-1}}, \\ \quad \vdots \qquad \vdots \qquad \vdots \\ f_{\lambda-1} = r_{\lambda-1}^{n_1}.r_\lambda^{n_2}\dots r_{\lambda-3}^{n_{\lambda-1}}, \\ f_\lambda \quad = r_\lambda^{n_1} \;.r_1^{n_2}\dots r_{\lambda-2}^{n_{\lambda-1}}. \end{cases}$$

Quod systema $\lambda-1$ aequationum atque $\lambda-1$ indeterminatarum n est, nam aequationibus omnibus multiplicatis per condicionem $f_1 f_2 \dots f_\lambda = r_1 r_2 \dots r_\lambda = 1$ aequationem identicam $1 = 1$ obtinemus, unde sequitur, ut quaevis istarum

aequationum e $\lambda-1$ reliquis deduci possit. Quodsi in systemate (II) logarithmos pro numeris adhibemus atque signis $\log f_k = \varphi_k$, $\log r_k = \varrho_k$ valores logarithmorum naturalium denotamus, obtinetur:

$$\text{(III.)}\quad \begin{cases} \varphi_1 = n_1\varrho_1+n_2\varrho_2+\cdots+n_{\lambda-1}\varrho_{\lambda-1}, \\ \varphi_2 = n_1\varrho_2+n_2\varrho_3+\cdots+n_{\lambda-1}\varrho_{\lambda}, \\ \vdots \qquad \vdots \qquad \vdots \qquad \vdots \\ \varphi_\lambda = n_1\varrho_\lambda+n_2\varrho_1+\cdots+n_{\lambda-1}\varrho_{\lambda-2}. \end{cases}$$

Quibus aequationibus deinceps per $1, \alpha, \alpha^2, \ldots \alpha^{\lambda-1}$ multiplicatis (ubi α radix aliqua unitatis λ^{ta} est) iisque additis eadem qua in § 1 usi sumus ratione obtinemus:

$$\text{(IV.)}\quad \varphi_1+\varphi_2\alpha+\cdots+\varphi_\lambda\alpha^{\lambda-1} = (n_1+n_2\alpha^{-1}+\cdots+n_{\lambda-1}\alpha^{-(\lambda-2)}).(\varrho_1+\varrho\ \alpha+\cdots+\varrho_\lambda\alpha^{\lambda-1}).$$

Iam positis:

$$\varphi_1+\varphi_2\alpha+\varphi_3\alpha^2+\cdots+\varphi_\lambda\alpha^{\lambda-1} = \varphi(\alpha),$$
$$\varrho_1+\varrho_2\alpha+\varrho_3\alpha^2+\cdots+\varrho_\lambda\alpha^{\lambda-1} = \varrho(\alpha)$$

erit

$$\varphi(\alpha) = \varrho(\alpha)(n_1+n_2\alpha^{-1}+\cdots+n_{\lambda-1}\alpha^{-(\lambda-2)}),$$

ergo:

$$\text{(V.)}\quad \frac{\varphi(\alpha).\varrho(\alpha^2).\varrho(\alpha^3)\ldots\varrho(\alpha^{\lambda-1})}{\varrho(\alpha).\varrho(\alpha^2).\varrho(\alpha^3)\ldots\varrho(\alpha^{\lambda-1})} = n_1+n_2\alpha^{-1}+\cdots+n_{\lambda-1}\alpha^{-(\lambda-2)},$$

quae aequatio systematis (III) solutionem repraesentat. Etenim posito brevitatis causa:

$$\frac{\varphi(\alpha).\varrho(\alpha^2)\ldots\varrho(\alpha^{\lambda-1})}{\varrho(\alpha).\varrho(\alpha^2)\ldots\varrho(\alpha^{\lambda-1})} = \psi(\alpha)$$

atque designante α radicem unitatis λ^{tam} ***primitivam*** aequatio (V) locum tenet aequationum:

$$\psi(\alpha^k) = n_1+n_2\alpha^{-k}+\cdots+n_{\lambda-1}\alpha^{-k(\lambda-2)} \qquad (k=1, 2, \ldots \lambda-1).$$

Unde (sicut pag. 4) colligimus esse:

$$\alpha^k\psi(\alpha)+\alpha^{2k}\psi(\alpha^2)+\cdots+\alpha^{(\lambda-1)k}\psi(\alpha^{\lambda-1}) = \lambda n_{k+1}-(n_1+n_2+\cdots+n_{\lambda-1})$$

pro valoribus $k=0, 1, \ldots \lambda-2$ et

$$\alpha^{\lambda-1}\psi(\alpha)+\alpha^{2(\lambda-1)}\psi(\alpha^2)+\cdots+\alpha^{(\lambda-1)^2}\psi(\alpha^{\lambda-1}) = -(n_1+n_2+\cdots+n_{\lambda-1}),$$

ergo denique:

$$\text{(VI.)}\quad \lambda n_{k+1} = (\alpha^k-\alpha^{-1})\psi(\alpha)+(\alpha^{2k}-\alpha^{-2})\psi(\alpha^2)+\cdots+(\alpha^{(\lambda-1)k}-\alpha)\psi(\alpha^{\lambda-1}),$$

qua aequatione re vera quodvis n quantitatibus ϱ et φ expressum est.

Sed etiam determinantem systematis (III) non evanescere demonstrandum est. Qui determinans denominator sinistrae partis aequationis (V)

scilicet productum

$$\varrho(\alpha).\varrho(\alpha^2)\ldots\varrho(\alpha^{\lambda-1})$$

est, designante α radicem primitivam. Ergo probandum est, nullum istius producti factorem evanescere, seu quantitatem

$$\varrho_1+\varrho_2\alpha+\varrho_3\alpha^2+\cdots+\varrho_\lambda\alpha^{\lambda-1} \quad \text{i. e.} \quad \sum_{k=0}^{k=\lambda-1}\varrho_{k+1}\alpha^k$$

pro quavis unitatis radice λ^{ta} unitate excepta a nihilo diversam esse. — Iam substituto ipsius ϱ_{k+1} valore scilicet:

$$\varrho_{k+1}=\log r_{k+1}=\log\frac{(1-\omega^{g^{k+1}})(1-\omega^{g^{k+1+\lambda}})\ldots(1-\omega^{g^{k+1+(\mu-1)\lambda}})}{(1-\omega^{g^k})\;(1-\omega^{g^{k+\lambda}})\;\ldots(1-\omega^{g^{k+(\mu-1)\lambda}})}$$

sive:

$$\begin{aligned}\varrho_{k+1} \;=\; &\log(1-\omega^{g^{k+1}})+\log(1-\omega^{g^{k+1+\lambda}})+\cdots+\log(1-\omega^{g^{k+1+(\mu-1)\lambda}})\\ &-\log(1-\omega^{g^k})\;-\log(1-\omega^{g^{k+\lambda}})\;-\cdots-\log(1-\omega^{g^{k+(\mu-1)\lambda}})\end{aligned}$$

$\varrho(\alpha)$ sive $\Sigma\varrho_{k+1}\alpha^k$ abit in:

$$\left\{\begin{aligned}&\sum_0^{\lambda-1}\{\log(1-\omega^{g^{k+1}})+\log(1-\omega^{g^{k+1+\lambda}})+\cdots+\log(1-\omega^{g^{k+1+(\mu-1)\lambda}})\}\,\alpha^k\\ -&\sum_0^{\lambda-1}\{\log(1-\omega^{g^k})\;+\log(1-\omega^{g^{k+\lambda}})\;+\cdots+\log(1-\omega^{g^{k+(\mu-1)\lambda}})\}\,\alpha^k\end{aligned}\right.$$

sive

$$\sum_{k=0}^{k=\mu\lambda-1}\alpha^k.\log(1-\omega^{g^{k+1}})-\sum_{k=0}^{k=\mu\lambda-1}\alpha^k.\log(1-\omega^{g^k}),$$

ratione scilicet habita aequationis $\alpha^{k+s\lambda}=\alpha^k$.

Iam cum sit:

$$-\log(1-\omega^{g^k}) \;=\; \frac{\omega^{g^k}}{1}+\frac{\omega^{2g^k}}{2}+\frac{\omega^{3g^k}}{3}+\cdots,$$

fit:

$$-\sum_0^{\mu\lambda-1}\alpha^k\log(1-\omega^{g^k}) \;=\; \sum_n\sum_{k=0}^{k=\mu\lambda-1}\alpha^k.\frac{\omega^{ng^k}}{n},$$

in qua summatione n omnes numeros integros positivos ad numerum ν primos designat. Nam pro valoribus $n=r\nu$ fit:

$$\omega^{ng^k}=1 \text{ et }\sum_0^{\mu\lambda-1}\frac{\alpha^k}{n}=\frac{1}{n}(1+\alpha+\alpha^2+\cdots+\alpha^{\mu\lambda-1})=0.$$

Quodsi Cli. *Jacobi* signis utimur, expressio

$$\sum_n\sum_0^{\mu\lambda-1}\alpha^k.\frac{\omega^{ng^k}}{n} \quad \text{abit in} \quad \sum_n\frac{1}{n}(\alpha,\omega^n),$$

ubi

$$(\alpha,\omega) \;=\; \omega+\alpha\,\omega^g+\alpha^2\omega^{g^2}+\cdots+\alpha^{\nu-2}\omega^{g^{\nu-2}},$$

et adhibita relatione $(\alpha, \omega^n) = \alpha^{-\mathrm{Ind.}n}(\alpha, \omega)$ obtinemus:

$$-\Sigma\alpha^k.\log(1-\omega^{g^k}) = (\alpha, \omega)\Sigma\frac{\alpha^{-\mathrm{Ind.}n}}{n}$$

et mutato ω in ω^g:

$$\Sigma\alpha^k.\log(1-\omega^{g^{k+1}}) = -(\alpha, \omega^g)\Sigma\frac{\alpha^{-\mathrm{Ind.}n}}{n}$$

i. e.

$$\Sigma\alpha^k.\log(1-\omega^{g^{k+1}}) = -\alpha^{-1}(\alpha, \omega).\Sigma\frac{\alpha^{-\mathrm{Ind.}n}}{n}.$$

Ergo habemus denique:

$$\varrho(\alpha) = (1-\alpha^{-1})(\alpha, \omega)\sum_n\frac{\alpha^{-\mathrm{Ind.}n}}{n}.$$

Iam neque factor (α, ω) neque $(1-\alpha^{-1})$ evanescere potest. Prior enim sententia ex aequatione $(\alpha, \omega)(\alpha^{-1}, \omega) = \pm\nu$, secunda ex eo, quod α ab unitate diversum positum est, elucet. Restat igitur, ut factorem $\Sigma\frac{\alpha^{-\mathrm{Ind.}n}}{n}$ non evanescere probetur. Tum etiam $\Sigma\frac{\alpha^{+\mathrm{Ind.}n}}{n}$ evanescere deberet, id quod pro nullo α, quod sit radix aequationis $x^{\nu-1} = 1$, ideoque etiam pro nulla radice unitatis λ^{ta} α fieri posse Cl. *Lejeune-Dirichlet* in illustri illa commentatione „de progressione arithmetica infinita“ etc. (§ 4 et 5) singularibus illis methodis demonstravit.

§ 10.

Si in valoribus quantitatum n, aequatione IV § 9 determinatis, numeros integros quam maximos secernimus, ita ut sint $n_1 = E_1 + \delta_1$, $n_2 = E_2 + \delta_2$, ..., quantitatibus δ inter 0 et 1 acceptis, aequationes II § 9 mutantur in:

$$\text{(I.)} \quad f_1 = r_1^{E_1}.r_2^{E_2}\ldots r_{\lambda-1}^{E_{\lambda-1}}.r_1^{\delta_1}r_2^{\delta_2}\ldots r_{\lambda-1}^{\delta_{\lambda-1}} \quad \text{etc.}$$

Ex quibus aequationibus, cum et f_1 et $r_1^{E_1}.r_2^{E_2}\ldots r_{\lambda-1}^{E_{\lambda-1}}$ unitates integrae complexae sint, alter quoque dextrae partis factor: $r_1^{\delta_1}.r_2^{\delta_2}\ldots r_{\lambda-1}^{\delta_{\lambda-1}}$ unitas integra complexa sit oportet. Ponatur igitur:

$$\text{(II.)} \quad \begin{cases} r_1^{\delta_1}r_2^{\delta_2}\ldots r_{\lambda-1}^{\delta_{\lambda-1}} = F_1 = A\varepsilon + A_1\varepsilon_1 + \cdots + A_{\lambda-1}\varepsilon_{\lambda-1}, \\ r_2^{\delta_1}r_3^{\delta_2}\ldots r_{\lambda}^{\delta_{\lambda-1}} = F_2 = A\varepsilon_1 + A_1\varepsilon_2 + \cdots + A_{\lambda-1}\varepsilon, \\ \quad\vdots \qquad\qquad \vdots \qquad\qquad \vdots \\ r_\lambda^{\delta_1}r_1^{\delta_2}\ldots r_{\lambda-2}^{\delta_{\lambda-1}} = F_\lambda = A\varepsilon_{\lambda-1} + A_1\varepsilon + \cdots + A_{\lambda-1}\varepsilon_{\lambda-2} \end{cases}$$

designantibus A, A_1, ... numeros integros. Quo facto secundum aequationes

illas VII § 1 has quae sequuntur aequationes tanquam istius systematis aequationum II solutionem nanciscimur:

$$\text{(III.)}\quad\begin{cases} -\nu.A = F_1(\mu-\varepsilon) + F_2(\mu-\varepsilon_1)+\cdots+F_\lambda(\mu-\varepsilon_{\lambda-1}),\\ -\nu.A_1 = F_1(\mu-\varepsilon_1) + F_2(\mu-\varepsilon_2)+\cdots+F_\lambda(\mu-\varepsilon),\\ \quad\vdots \qquad\qquad \vdots \qquad\qquad \vdots\\ -\nu.A_{\lambda-1} = F_1(\mu-\varepsilon_{\lambda-1})+F_2(\mu-\varepsilon)+\cdots+F_\lambda(\mu-\varepsilon_{\lambda-2}).\end{cases}$$

Periodos ε minores esse numero μ, quo numerum terminorum periodi designavimus, facile perspicitur. Nam quaevis periodus ε (posito $\frac{1}{2}\mu = \mathfrak{m}$) formae est:

$$\omega^{k_1}+\omega^{-k_1}+\omega^{k_2}+\omega^{-k_2}+\cdots+\omega^{k_\mathfrak{m}}+\omega^{-k_\mathfrak{m}}$$

sive igitur formae

$$2\cdot\left\{\cos\frac{2k_1\pi}{\nu}+\cos\frac{2k_2\pi}{\nu}+\cdots+\cos\frac{2k_\mathfrak{m}\pi}{\nu}\right\},$$

quod aggregatum cosinuum ipsorum numero $\frac{1}{2}\mu$ minus esse in promptu est.

Deinde absolutos ipsorum F valores limites quosdam $\mathfrak{F}_1$, $\mathfrak{F}_2$, ... superare non posse ex aequationibus II et condicionibus, quibus ibidem quantitates δ sunt circumscriptae, colligi potest. Unde sequitur, ut quantitates quoque $-\nu A$, $-\nu A_1$, ... limitibus quibusdam contineantur, scilicet cum quantitates $\mu-\varepsilon$ sint positivae:

$$\mathfrak{F}_1(\mu-\varepsilon_k)+\mathfrak{F}_2(\mu-\varepsilon_{k+1})+\cdots+\mathfrak{F}_\lambda(\mu-\varepsilon_{k-1}) > -\nu A_k,$$
$$-\mathfrak{F}_1(\mu-\varepsilon_k)-\mathfrak{F}_2(\mu-\varepsilon_{k+1})-\cdots-\mathfrak{F}_\lambda(\mu-\varepsilon_{k-1}) < -\nu A_k,$$

sive

$$\frac{1}{\nu}\{\mathfrak{F}_1(\mu-\varepsilon_k)+\cdots+\mathfrak{F}_\lambda(\mu-\varepsilon_{k-1})\} > A_k > -\frac{1}{\nu}\{\mathfrak{F}_1(\mu-\varepsilon_k)+\cdots+\mathfrak{F}_\lambda(\mu-\varepsilon_{k-1})\}.$$

Cum vero A_k numerus integer esse debeat, multitudinem tantum finitam numerorum A, A_1, ... etiamque igitur numerum finitum unitatum F, quae forma in II accepta gaudeant, existere posse patet.

Quae cum conferamus cum aequatione I, sequitur, ut quaelibet unitas f potestatibus integris unitatum coniunctarum r_1, r_2, ... $r_{\lambda-1}$ et unitatibus quibusdam numeri finiti exprimi possint; i. e. ut cunctae unitates forma

$$F.r_1^{k_1}.r_2^{k_2}\ldots r_{\lambda-1}^{k_{\lambda-1}}$$

contineantur, designantibus k_1, k_2, ... numeros integros et F unitatem quandam e numero unitatum finito electam, sive denique ut numerus unitatum fundamentalium, quarum potestatibus integris omnis unitas repraesentari queat, finitus sit.

§ 11.

Iam accuratius, quibus limitibus numeri integri $A, A_1, \ldots$ sint circumscripti, consideraturi sumus, quo labor inveniendi unitates fundamentales aliquanto diminuatur. Ad quem finem disquisitionem instituamus de illa expressione ipsius $-\nu A_k$ (§ 10, III):

$$\text{(I.)} \quad F_1(\mu-\varepsilon_k)+F_2(\mu-\varepsilon_{k+1})+\cdots+F_\lambda(\mu-\varepsilon_{k-1}),$$

ubi

$$F_n = r_n^{\delta_1}.r_{n+1}^{\delta_2}\ldots r_{n-2}^{\delta_{\lambda-1}},$$

eamque consideremus tanquam functionem quantitatum δ. Quotientes differentiales istius functionis 1 respectu quantitatum $\delta_1, \delta_2, \ldots$ sunt:

$$\text{(II.)} \quad \begin{cases} F_1(\mu-\varepsilon_k)\varrho_1 \quad +F_2(\mu-\varepsilon_{k+1})\varrho_2+\cdots+F_\lambda(\mu-\varepsilon_{k-1})\varrho_\lambda, \\ F_1(\mu-\varepsilon_k)\varrho_2 \quad +F_2(\mu-\varepsilon_{k+1})\varrho_3+\cdots+F_\lambda(\mu-\varepsilon_{k-1})\varrho_1, \\ \quad\vdots \qquad\qquad \vdots \qquad\qquad \vdots \qquad\qquad , \\ F_1(\mu-\varepsilon_k)\varrho_{\lambda-1}+F_2(\mu-\varepsilon_{k+1})\varrho_\lambda+\cdots+F_\lambda(\mu-\varepsilon_{k-1})\varrho_{\lambda-2}, \end{cases}$$

in quibus formulis notatione iam supra adhibita, $\log r_k = \varrho_k$, usi sumus.

Quotientes differentiales secundi et quidem ii, quos expressionum (II) prima respectu δ_1, secunda respectu δ_2 etc. differentiatis obtinemus, erunt:

$$\begin{cases} F_1(\mu-\varepsilon_k)\varrho_1^2 \quad +F_2(\mu-\varepsilon_{k+1})\varrho_2^2+\cdots+F_\lambda(\mu-\varepsilon_{k-1})\varrho_\lambda^2, \\ F_1(\mu-\varepsilon_k)\varrho_2^2 \quad +F_2(\mu-\varepsilon_{k+1})\varrho_3^2+\cdots+F_\lambda(\mu-\varepsilon_{k-1})\varrho_1^2, \\ \quad\vdots \qquad\qquad \vdots \qquad\qquad \vdots \qquad\qquad , \\ F_1(\mu-\varepsilon_k)\varrho_{\lambda-1}^2+F_2(\mu-\varepsilon_{k+1})\varrho_\lambda^2+\cdots+F_\lambda(\mu-\varepsilon_{k-1})\varrho_{\lambda-2}^2, \end{cases}$$

quas expressiones pro quibusvis quantitatum δ valoribus positivas manere elucet. Unde facili consideratione colligi potest, functionem illam (I), dum variabiles δ intervallum inter 0 et 1 percurrunt, valorem haud maiorem obtinere posse eo, qui inter valores functionis extremis ipsorum δ valoribus respondentes maximus sit. Quare quaestio de valore ipsius νA_k absolute maximo ad disquisitionem valorum, qui ad valores quantitatum δ hos: 0 et 1 pertinent, restringitur. Valoribus igitur quantitatum r computatis, quantitates F combinationibus quibusvis valorum 0 et 1 pro ipsis δ (multitudinis igitur $2^{\lambda-1}$) respondentes computentur, ut valor earum maximus M inveniatur. Sit numerus integer ipso $\frac{M}{\nu}$ minor eique proximus $= n$; iam unitates omnes complexae, quarum coefficientes inter $-n$ et $+n$ sunt, statuendae atque inter eas, quae ad alias reduci possunt, reiiciendae, ut tandem numerus unitatum fundamentalium quam minimus restet.

Sic e. g. posito $\nu = 7$, $\lambda = 3$ atque

$$r_1 = \omega + \omega^{-1}, \quad r_2 = \omega^2 + \omega^{-2}, \quad r_3 = \omega^3 + \omega^{-3}$$

iste numerus $n = 1$ sine magno labore invenitur, ita ut valores coefficientium sint -1, 0, $+1$. Numeri igitur complexi 24 disquirendi *), inter quos vero terni factores sunt coniuncti. Inter octo illos, qui supersunt, rursus bini numeros aequales sed signo tantum oppositos praebent, ita ut denique hi quatuor restent:

$$\varepsilon_1 = \omega + \omega^{-1},$$
$$\varepsilon_1 + \varepsilon_2 = \omega + \omega^{-1} + \omega^2 + \omega^{-2} = \varepsilon_2 . \varepsilon_3,$$
$$\varepsilon_1 + \varepsilon_2 - \varepsilon_3 = \omega + \omega^{-1} + \omega^2 + \omega^{-2} - \omega^3 - \omega^{-3} = -\varepsilon_2 . \varepsilon_3^3,$$

$\varepsilon_1 - \varepsilon_2$ unitas complexa non est.

Cumque tres illas unitates unitatibus ipsis ε exprimere liceat, has ipsas tanquam fundamentales accipere possumus, i. e. quarum potestatibus integris omnes unitates complexae ad $\nu = 7$, $\lambda = 3$ pertinentes repraesentari possint.

Haud inutile videtur hoc ipsum exemplum paulo uberius exponere, ut id de quo agitur magis in promptu sit. Cum enim sit:

$$\mathrm{Nm}(x\varepsilon + y\varepsilon_1 + z\varepsilon_2) = (x + y + z)^3 - 7(xy^2 + yz^2 + zx^2 + xyz),$$

solutionem aequationis

$$(x + y + z)^3 - 7(xy^2 + yz^2 + zx^2 + xyz) = \pm 1$$

numeris integris ita invenimus, ut numeri x, y, z integri determinentur aequationibus **):

$$\begin{cases} -7x = (\omega+\omega^{-1})^m(\omega^2+\omega^{-2})^n(2-\omega-\omega^{-1}) + (\omega^2+\omega^{-2})^m(\omega^3+\omega^{-3})^n(2-\omega^2-\omega^{-2}) \\ \qquad\qquad + (\omega^3+\omega^{-3})^m(\omega+\omega^{-1})^n(2-\omega^3-\omega^{-3}), \\ -7y = (\omega+\omega^{-1})^m(\omega^2+\omega^{-2})^n(2-\omega^2-\omega^{-2}) + (\omega^2+\omega^{-2})^m(\omega^3+\omega^{-3})^n(2-\omega^3-\omega^{-3}) \\ \qquad\qquad + (\omega^3+\omega^{-3})^m(\omega+\omega^{-1})^n(2-\omega-\omega^{-1}), \\ -7z = (\omega+\omega^{-1})^m(\omega^2+\omega^{-2})^n(2-\omega^3-\omega^{-3}) + (\omega^2+\omega^{-2})^m(\omega^3+\omega^{-3})^n(2-\omega-\omega^{-1}) \\ \qquad\qquad + (\omega^3+\omega^{-3})^m(\omega+\omega^{-1})^n(2-\omega^2-\omega^{-2}), \end{cases}$$

designantibus m, n quoslibet numeros integros. Quod exemplum analogiam aequationis Pellianae prae se ferre apparet.

---

*) Nempe omissis his: 0, $\varepsilon_1 + \varepsilon_2 + \varepsilon_3$, $-\varepsilon_1 - \varepsilon_2 - \varepsilon_3$.

**) v. III. § 10.

§ 12.

Postquam demonstravimus numerum unitatum fundamentalium finitum esse, de hoc ipso numero disquisitiones instituamus ac primum quidem illum numerum ipso $\lambda-1$ minorem esse non posse sumus probaturi.

Sint igitur unitates fundamentales: $f, f', f'', \ldots$, quarum logarithmi resp. literis $\varphi, \varphi', \varphi'', \ldots$ designentur. Quodsi literis

$$r_1, \quad r_2, \quad \ldots \quad r_\lambda; \quad \varrho_1, \quad \varrho_2, \quad \ldots \quad \varrho_\lambda$$

eandem quam in paragraphis antecedentibus tribuimus vim, hae ipsae unitates potestatibus integris ipsorum f exprimi possint oportet. Quare sit:

$$\begin{array}{ll} r_1 = f^{a_1} . f'^{b_1} . f''^{c_1} \ldots, & \varrho_1 = a_1\varphi + b_1\varphi' + c_1\varphi'' + \cdots, \\ r_2 = f^{a_2} . f'^{b_2} . f''^{c_2} \ldots, & \varrho_2 = a_2\varphi + b_2\varphi' + c_2\varphi'' + \cdots, \\ \vdots & \vdots \\ r_{\lambda-1} = f^{a_{\lambda-1}} . f'^{b_{\lambda-1}} . f''^{c_{\lambda-1}} \ldots, & \varrho_{\lambda-1} = a_{\lambda-1}\varphi + b_{\lambda-1}\varphi' + c_{\lambda-1}\varphi'' + \cdots. \end{array}$$

Cum vero numerus quantitatum φ sit $\leqq \lambda-2$, his ipsis eliminatis certe una restabit aequatio formae:

$$\text{(I.)} \qquad n_1\varrho_1 + n_2\varrho_2 + \cdots + n_{\lambda-1}\varrho_{\lambda-1} = 0,$$

in qua aequatione $n_1, n_2, \ldots$ non omnes nihilo aequales atque numeri integri esse deberent, cum et ipsa $a, b, c, \ldots$ numeri sint integri. Id quod esse non posse sequentibus probatur.

Ex aequatione enim (I) colligimus aequationem:

$$r_1^{n_1} . r_2^{n_2} \ldots r_{\lambda-1}^{n_{\lambda-1}} = 1,$$

unde rursus mutatis periodis, quae expressionibus r continentur, hoc oritur aequationum systema:

$$\begin{array}{l} r_1^{n_1} r_2^{n_2} \ldots r_{\lambda-1}^{n_{\lambda-1}} = 1, \\ r_2^{n_1} r_3^{n_2} \ldots r_\lambda^{n_{\lambda-1}} = 1, \\ \vdots \\ r_\lambda^{n_1} r_1^{n_2} \ldots r_{\lambda-2}^{n_{\lambda-1}} = 1. \end{array}$$

Unde per aequationem (IV) § 9 obtinemus:

$$(n_1 + n_2\alpha^{-1} + \cdots + n_{\lambda-1}\alpha^{-(\lambda-2)})(\varrho_1 + \varrho_2\alpha + \cdots + \varrho_\lambda\alpha^{\lambda-1}) = 0$$

pro quoque ipsius α valore. Cum autem factorem secundum non evanescere iam supra (§ 9) demonstratum sit, factor prior pro quoque ipsius α valore unitate excepta evanescere deberet, id quod fieri nequit, nisi $n_1 = n_2 = \cdots = 0$.

§ 13.

Antequam vero ad ulteriorem disquisitionem accedamus, minime a re abhorrere videtur notationem quandam indicare, qua formulae magnopere contrahantur. Designantibus enim $r_1, r_2, \ldots r_{\lambda-1}, r_\lambda$ unitates aliquas coniunctas, denotamus productum:

$$r_1^{n_1}.r_2^{n_2}\ldots r_{\lambda-1}^{n_{\lambda-1}}$$

signo:

$$r_1^{n_1+n_2\alpha+\cdots+n_{\lambda-1}\alpha^{\lambda-2}} \text{ sive } r_1^{n(\alpha)}.$$

Id quod ita quoque exhiberi potest, ut dicamus, posito

$$r_1^{n_1}.r_2^{n_2}\ldots r_{\lambda-1}^{n_{\lambda-1}} = f_1,$$

pro aequationibus illis (IV § 9):

$$\varphi(\alpha^k) = (n_1+n_2\alpha^{-k}+\cdots+n_{\lambda-1}\alpha^{-k(\lambda-2)})\varrho(\alpha^k)$$

substitui aequationem:

$$f_1 = r_1^{n_1+n_2\alpha+\cdots+n_{\lambda-1}\alpha^{\lambda-2}}.$$

Iam primum adnotandum est, productum $r_1^{n_1}.r_2^{n_2}\ldots r_\lambda^{n_\lambda}$ aequatione

$$r_1.r_2\ldots r_\lambda = 1$$

ad productum $\lambda-1$ terminorum pariterque numerum complexum $n(\alpha)$ ope aequationis

$$1+\alpha+\alpha^2+\cdots+\alpha^{\lambda-1} = 0$$

ad expressionem $\lambda-1$ terminorum redigi posse.

E definitione statim sequuntur aequationes:

$$r_1^{n(\alpha)} = r_2^{\alpha^{-1}n(\alpha)} = r_3^{\alpha^{-2}n(\alpha)} = \cdots = r_\lambda^{\alpha^{-(\lambda-1)}n(\alpha)},$$

$$r_1^{m(\alpha)+n(\alpha)} = r_1^{m(\alpha)}.r_1^{n(\alpha)}.$$

Etiamque altera verarum potestatum virtute hoc nostrum symbolum gaudet, scilicet:

$$[r_1^{n(\alpha)}]^{m(\alpha)} = r_1^{n(\alpha).m(\alpha)}.$$

Posito enim

$$r_1^{n(\alpha)} = s_1 \quad \text{et} \quad [r_1^{n(\alpha)}]^{m(\alpha)} = s_1^{m(\alpha)} = t_1$$

habemus aequationes:

$$r_1^{n_1}.r_2^{n_2}\cdots = s_1, \quad r_2^{n_1}.r_3^{n_2}\cdots = s_2, \quad \ldots,$$

quae posito $\log s_k = \sigma_k$ secundum § 9, (II), (III), (IV) eandem habent vim

quam aequatio:

$$n(\alpha^{-1})\varrho(\alpha) = \sigma(\alpha),$$

quae ipsa, ut supra, aequationum $\lambda-1$ locum tenet. Eodem modo est:

$$m(\alpha^{-1}).\sigma(\alpha) = \tau(\alpha), \quad \text{ergo} \quad n(\alpha^{-1}).m(\alpha^{-1})\varrho(\alpha) = \tau(\alpha),$$

pro qua igitur aequatione, quod ad definitionem nostram, substituere possumus hanc: $t_1 = r_1^{n(\alpha).m(\alpha)}$ q. e. d.

Iam patet, posito λ numerum primum esse, istos exponentes symbolicos sicuti numeros complexos tractari posse, cum omnes eorum reductiones eo tantum nitantur, ut sit:

$$1+\alpha+\alpha^2+\cdots+\alpha^{\lambda-1} = 0,$$

id quod cum nostra definitione consentit, scilicet

$$r_1^{1+\alpha+\cdots+\alpha^{\lambda-1}} = r_1.r_2\ldots r_\lambda = 1 = r_1^0.$$

Deinde praemittendum est, literis r illa priore vi gaudentibus, cum nullum factorem $\varrho(\alpha)$ evanescere demonstratum sit, unitates $r_1^{n(\alpha)}$ et $r_1^{m(\alpha)}$ aequales esse non posse nisi $n_1 = m_1$, $n_2 = m_2$, ..., $n_{\lambda-1} = m_{\lambda-1}$ i. e. nisi $n(\alpha) = m(\alpha)$ pro omnibus λ^{tis} unitatis radicibus excepta unitate.

Demonstravimus in § 9 quamvis unitatem complexam forma

$$r_1^{n_1}.r_2^{n_2}\ldots r_{\lambda-1}^{n_{\lambda-1}}$$

contineri, quae quantitates n etiam loco citato determinatae sunt. Iam vero istas quantitates rationales esse probabimus. — Etenim initio § 10, posita unitate integra complexa

$$f_1 = r_1^{n_1}.r_2^{n_2}\ldots r_{\lambda-1}^{n_{\lambda-1}},$$

etiam productum

$$r_1^{\delta_1}.r_2^{\delta_2}\ldots r_{\lambda-1}^{\delta_{\lambda-1}}$$

unitatem integram esse ostendimus, si quantitates δ residua sunt ipsorum n numero integro quam maximo subtracto. Cum vero quivis numerus irrationalis, variis numeris integris multiplicatus, innumera praebeat residua unitate minora eaque inter se diversa, cumque unitas f ad potestatem aliquam integram evecta rursus unitas integra sit, variis potestatibus integris unitatis f innumeras unitates inter se diversas formae

$$r_1^{\delta_1}.r_2^{\delta_2}\ldots r_{\lambda-1}^{\delta_{\lambda-1}}$$

(ubi δ_1, δ_2, ... < 1) obtineri posse elucet. Illo autem § 10 finitum tantummodo numerum unitatum complexarum huius formae existere demonstravimus;

id quod itaque a propositione nostra, quantitates n irrationales esse, abhorret. — Quod cum conferamus cum forma § 10 (sub finem) omnes unitates formae esse patet:

$$r_1^{\frac{m(\alpha)}{n}} . r_1^{k(\alpha)},$$

designantibus $m(\alpha)$, $k(\alpha)$ numeros integros complexos, n numerum realem, in qua quidem numerus fractionum diversarum $\frac{m(\alpha)}{n}$ finitus est.

§ 14.

Iam primum ad casum simpliciorem accedamus, in quo scilicet λ numerus primus ponitur. Quem quoque talem supponimus, ut quivis numerus formae $k\lambda+g^d$ (designante d divisorem numeri $\lambda-1$) in d factores complexos dissolvi queat (v. § 6).

Cum secundum supra dicta numerus unitatum formae $r^{\frac{m(\alpha)}{n}}$ (quibus praeter ipsas r ad repraesentandas omnes opus sit) finitus sit, hae ipsae sint:

$$\text{(I.)} \quad r^{\frac{m(\alpha)}{n}}, \quad r^{\frac{m'(\alpha)}{n'}}, \quad \ldots .$$

Iam sit factor numerorum $m(\alpha)$ et n communis maximus $v(\alpha)$*), ita ut

$$m(\alpha) = a(\alpha).v(\alpha), \quad n = c(\alpha).v(\alpha),$$

loco illius exponentis $\frac{m(\alpha)}{n}$ scribere licet hunc: $\frac{a(\alpha)}{c(\alpha)}$. Cumque $a(\alpha)$ et $c(\alpha)$ nullum amplius factorem communem habeant, numerus inveniri potest $b(\alpha)$ talis, ut sit (v. § 4)

$$b(\alpha).a(\alpha) \equiv 1 \pmod{c(\alpha)}$$

sive

$$b(\alpha).a(\alpha) = 1+F(\alpha).c(\alpha).$$

Cum vero $r^{\frac{m(\alpha)}{n}}$ sive $r^{\frac{a(\alpha)}{c(\alpha)}}$ unitas integra sit, eadem proprietate unitatem $r^{\frac{a(\alpha).b(\alpha)}{c(\alpha)}}$ sive $r^{\frac{1}{c(\alpha)}}.r^{F(\alpha)}$ ideoque etiam unitatem $r^{\frac{1}{c(\alpha)}}$ gaudere patet. De qua unitate cum illa unitas data deduci possit, scilicet evehendo eam ad potestatem integram $a(\alpha)$, hanc ipsam loco illius accipere convenit. Hinc elucet, pro illis unitatibus (I) accipi posse unitates huius formae:

$$\text{(II.)} \quad r^{\frac{1}{n(\alpha)}}, \quad r^{\frac{1}{n'(\alpha)}}, \quad \ldots .$$

*) De factore communi maximo sermonem esse posse, e suppositione illa de natura ipsius λ facta elucet. (Cf. adnotatio ad. § 4).

Ut harum unitatum binae in unam conflentur, sit factor numerorum $n(\alpha)$ et $n'(\alpha)$ communis maximus $c(\alpha)$, ita ut sit

$$n(\alpha) = c(\alpha).m(\alpha), \quad n'(\alpha) = c(\alpha).m'(\alpha).$$

Iam cum numeri $m(\alpha)$ et $m'(\alpha)$ nullum amplius habeant factorem communem, numerus inveniri potest $a(\alpha)$ talis, ut sit (v. § 4)

$$a(\alpha).m(\alpha) \equiv 1 \ (\text{mod.}\, m'(\alpha))$$

sive

$$a(\alpha).m(\alpha)+b(\alpha).m'(\alpha) = 1.$$

Cum vero unitates $r^{\frac{1}{n(\alpha)}}$ et $r^{\frac{1}{n'(\alpha)}}$ integrae sint, unitates quoque $r^{\frac{b(\alpha)}{n(\alpha)}}$ et $r^{\frac{a(\alpha)}{n'(\alpha)}}$ etiamque $r^{\frac{b(\alpha)}{n(\alpha)}}.r^{\frac{a(\alpha)}{n'(\alpha)}}$ sive $r^{\frac{b(\alpha)}{n(\alpha)}+\frac{a(\alpha)}{n'(\alpha)}}$ integras esse in promptu est. Est vero:

$$\frac{b(\alpha)}{n(\alpha)}+\frac{a(\alpha)}{n'(\alpha)} = \frac{1}{c(\alpha)}\left\{\frac{b(\alpha)}{m(\alpha)}+\frac{a(\alpha)}{m'(\alpha)}\right\} = \frac{1}{c(\alpha).m(\alpha).m'(\alpha)},$$

unde igitur unitatem $r^{\frac{1}{c(\alpha).m(\alpha).m'(\alpha)}}$ integram esse liquet. De qua cum illae unitates $r^{\frac{1}{n(\alpha)}}$ et $r^{\frac{1}{n'(\alpha)}}$ evehendo eam resp. ad potestates integras $m'(\alpha)$ et $m(\alpha)$ deduci possint, hanc ipsam loco illarum accipere licet. Qua ratione agendi iterata denique loco unitatum (I) vel (II) una restabit formae $r^{\frac{1}{\nu(\alpha)}}$, qua praeter unitates r ad repraesentandas omnes unitates opus erit. Quodsi $r^{\frac{1}{\nu(\alpha)}} = u$ ponimus, est $r = u^{\nu(\alpha)}$, ex qua aequatione, ut ipsae unitates r integris ipsorum u potestatibus exprimi possint, sequitur; ergo forma:

$$u_1^{n(\alpha)} = u_1^{n_1}.u_2^{n_2}\ldots u_{\lambda-1}^{n_{\lambda-1}},$$

designantibus n_1, n_2, ... $n_{\lambda-1}$ quoscunque numeros integros reales, omnes unitates integrae complexae eaeque solae continentur.

Postquam hanc methodum quasi geneticam exposuimus, aliam allaturi sumus rationem, quae huius paragraphi summam a posteriori probet.

§ 15.

Unitas r nisi ipsa fundamentalis est, praeter eas unitates, quae potestatibus ipsius r integris complexis repraesentari possunt, numerus finitus existet unitatum formae: $r^{\frac{m(\alpha)}{n}}$. Inter quas erit una quaedam (vel plures), in qua norma exponentis i. e. $\text{Nm}\frac{m(\alpha)}{n}$ reliquis minor est. Qualem unitatem

litera u designemus. Quae unitas eam habet proprietatem, ut si quae exstet unitas integra formae: $u^{\frac{h(\alpha)}{k}}$, norma exponentis i. e. $\mathrm{Nm}\frac{h(\alpha)}{k}$ unitate maior sit oporteat. Etenim cum

$$r^{\frac{m(\alpha)}{n}} = u$$

ideoque

$$r^{\frac{m(\alpha)}{n}\cdot\frac{h(\alpha)}{k}} = u^{\frac{h(\alpha)}{k}}$$

praetereaque $\mathrm{Nm}\frac{m(\alpha)}{n}\cdot\frac{h(\alpha)}{k} > \mathrm{Nm}\frac{m(\alpha)}{n}$ secundum suppositionem de unitate u factam esse debeat, illa condicio $\mathrm{Nm}\frac{h(\alpha)}{k} > 1$ sponte manat. — Iam demonstrabimus, unitatem u illa ratione electam fundamentalem esse, sive nullam existere unitatem integram, nisi quae eius potestate integra complexa repraesentari possit. Quodsi enim unitas exstet formae $u^{\frac{h(\alpha)}{k}}$ sive formae $u^{\frac{m(\alpha)}{n(\alpha)}}$, ubi numeros $m(\alpha)$ et $n(\alpha)$ omni factore communi carere supponere licet, numerus $a(\alpha)$ inveniri potest talis, ut sit (v. § 4)

$$a(\alpha)m(\alpha) \equiv 1 \pmod{n(\alpha)}.$$

Cum vero unitas $u^{\frac{m(\alpha)}{n(\alpha)}}$ ideoque $u^{a(\alpha)\frac{m(\alpha)}{n(\alpha)}}$ integra sit, ratione supra (§ 14) adhibita unitatem quoque $u^{\frac{1}{n(\alpha)}}$ integram esse colligimus. Ergo secundum supra exhibita $\mathrm{Nm}\frac{1}{n(\alpha)} \geqq 1$ esse debet i. e. $\mathrm{Nm}\,n(\alpha) \leqq 1$. Cum vero $\mathrm{Nm}\,n(\alpha)$ tanquam numerus integer unitate minor esse nequeat, tantum restat, ut sit $\mathrm{Nm}\,n(\alpha) = 1$, i. e. ut numerus $n(\alpha)$ unitas complexa sit. Unde ut fractio $\frac{m(\alpha)}{n(\alpha)}$ tanquam numerus complexus integer scribi possit atque igitur ut omnes unitates integrae potestatibus ipsius u integris complexis repraesentari possint sequitur.

§ 16.

Postquam ostendimus, existere unitates quasdam fundamentales numeri $\lambda-1$ easque coniunctas in numeris λ illa virtute initio § 14 memorata praeditis, de his ipsis quaedam adnotamus. Designentur unitates aliquae fundamentales ut supra literis: $u_1, u_2, \ldots u_{\lambda-1}$, has ipsas tales esse ostendimus, ut $u_1^{n(\alpha)}$ cunctas repraesentet unitates, posito $n(\alpha)$ numerum aliquem integrum complexum. Quaeque unitates u ea ipsa proprietate gaudent, fundamentales

sunt. Nunc designante $k(\alpha)$ unitatem aliquam complexam integram atque posito: $u_1^{k(\alpha)} = v_1$, aperte est:

$$u_1^{k(\alpha)k(\alpha^2)\dots k(\alpha^{\lambda-1})} = u_1 = v_1^{k(\alpha^2)\dots k(\alpha^{\lambda-1})} = v_1^{K(\alpha)},$$

quae aequatio ipsam unitatem u potestate integra complexa ipsius v repraesentat, unde hanc ipsam quoque unitatem v fundamentalem esse elucet. Sive posita aliqua unitate fundamentali u, omnes unitates fundamentales eaeque solae forma continentur: $u^{k(\alpha)}$, designante $k(\alpha)$ unitatem complexam. Hinc colligimus existere tot unitates fundamentales quot unitates diversae ex numeris integris et radicibus unitatis λ^{tis} compositae, ergo pro $\lambda = 2$ duae, pro $\lambda = 3$ sex, pro $\lambda \geqq 5$ numerus infinitus exstat unitatum fundamentalium coniunctarum. — Etiamque unitates $\lambda - 1$ non coniunctae statui possunt, quarum potestatibus integris cunctae repraesentari possunt unitates. Posito enim:

$$\begin{cases} u_1^{a_1}.u_2^{a_2}\dots u_{\lambda-1}^{a_{\lambda-1}} = A, \\ u_1^{b_1}.u_2^{b_2}\dots u_{\lambda-1}^{b_{\lambda-1}} = B, \\ \vdots \quad \vdots \quad \vdots, \end{cases}$$

designantibus $a, b, \dots$ numeros integros, obtinebimus aequationes $\lambda - 1$:

$$\begin{cases} a_1 \log u_1 + a_2 \log u_2 + \dots + a_{\lambda-1} \log u_{\lambda-1} = \log A, \\ b_1 \log u_1 + b_2 \log u_2 + \dots + b_{\lambda-1} \log u_{\lambda-1} = \log B, \\ \vdots \quad \vdots \quad \vdots \quad \vdots, \end{cases}$$

ex quo systemate quantitates $\log u_1$, $\log u_2$, ... determinari possunt, idque hac ratione:

$$\Delta . \log u_1 = m_1 . \log A + m_2 . \log B + \dots,$$

designante Δ determinantem illius systematis, m_1, m_2, ... numeros quosdam integros. Hinc iam patet, si systema istud ea gaudet proprietate, ut sit $\Delta = \pm 1$, unitates u ideoque omnes unitates potestatibus integris unitatum $A, B, \dots$ exprimi posse. Unde etiam tales unitates $A, B, \dots$ infinitis modis (dummodo $\lambda \geqq 3$) eligi posse, plane in promptu est.

Quae ut ad unum tantum exemplum adhibeamus, ponamus uti in § 11 $\nu = 7$, $\lambda = 3$. Loco citato ostendimus unitates: $u_1 = \omega + \omega^{-1}$, $u_2 = \omega^2 + \omega^{-2}$ sive $u_1 = \varepsilon_1$, $u_2 = \varepsilon_2$ fundamentales esse. Iam cum sint unitates pro $\lambda = 3$ sex scilicet:

$$1, \quad \alpha, \quad \alpha^2, \quad -1, \quad -\alpha, \quad -\alpha^2,$$

habemus sexies binas unitates coniunctas fundamentales:

$$\begin{array}{llll} u_1^1 \text{ ergo } \varepsilon_1, & \varepsilon_2, & u_1^{-1} \dots \varepsilon_1 + \varepsilon_2, & \varepsilon_2 + \varepsilon_3, \\ u_1^{\alpha} \ \dots \ \varepsilon_2, & \varepsilon_3, & u_1^{-\alpha} \dots \varepsilon_2 + \varepsilon_3, & \varepsilon_3 + \varepsilon_1, \\ u_1^{\alpha^2} \ \dots \ \varepsilon_3, & \varepsilon_1, & u_1^{-\alpha^2} \dots \varepsilon_3 + \varepsilon_1, & \varepsilon_1 + \varepsilon_2, \end{array}$$

deinde positis $u_1^{a_1}.u_2^{a_2} = A$, $u_1^{b_1}.u_2^{b_2} = B$, erit:

$$a_1 \log u_1 + a_2 \log u_2 = \log A,$$
$$b_1 \log u_1 + b_2 \log u_2 = \log B,$$

ideoque $\Delta = a_1 b_2 - a_2 b_1 = \pm 1$ condicio illa, ut unitates A et B partes unitatum fundamentalium agant. Cui aequationi innumeris modis satisfieri potest. E. g. positis:

$$a_1 = 3, \quad a_2 = 2, \quad b_1 = 4, \quad b_2 = 3$$

habemus ut unitates fundamentales:

$$A = u_1^3.u_2^2 = 5\varepsilon_1 + \varepsilon_2 + 3\varepsilon_3, \quad B = u_1^4.u_2^3 = 11\varepsilon_1 + 2\varepsilon_2 + 7\varepsilon_3.$$

§ 17.

Nunc omissa suppositione illa, qua statuitur, omnem numerum primum formae $k\lambda + g^h$ in h factores complexos discerpi posse, servata vero ea, qua λ numerum esse primum continetur, unitates investigemus.

Quodsi literis $r_1, r_2, \ldots r_{\lambda-1}$ aliquas unitates coniunctas*) designamus, quaevis unitas integris istius unitatis datae potestatibus repraesentari potest, adiuncto numero finito certarum quarundam fractarum ipsorum r potestatum. Quare sint cunctae unitates, quibus praeter ipsas r ad exprimendas omnes unitates opus sit:

$$\text{(I.)} \qquad r^{\frac{m(\alpha)}{n}}, \quad r^{\frac{m'(\alpha)}{n'}}, \quad \ldots .$$

Iam si $n = kl$ et numerus k ad numerum l primus est, existunt numeri g et h tales, ut sit

$$hk + gl = 1,$$

ergo

$$\frac{hk^2}{n} + g = \frac{1}{l}, \quad \frac{gl^2}{n} + h = \frac{1}{k};$$

quare loco unitatis $r^{\frac{m(\alpha)}{n}}$ accipi possunt unitates

$$r^{\frac{m(\alpha)}{k}}, \quad r^{\frac{m(\alpha)}{l}},$$

cum illa unitas $r^{\frac{m(\alpha)}{n}}$ tanquam productum

$$r^{g.\frac{m(\alpha)}{k}}.r^{h.\frac{m(\alpha)}{l}}$$

*) Quae vero tales esse debent, ut expressio illa $\mathrm{Nm}(\varrho_1 + \varrho_2\alpha + \cdots + \varrho_\lambda\alpha^{\lambda-1})$ non evanescat (cf. § 9).

repraesentari potest. Eadem ratione probari potest, pro istis unitatibus (I) accipi posse unitates huius formae

$$\text{(II.)}\quad r^{\frac{k(\alpha)}{p^a}},\quad r^{\frac{k'(\alpha)}{q^b}},\quad \ldots,$$

quorum exponentium numeratores et denominatores factores reales communes non habere supponimus. Sit vero summa ipsius p potestas, qua numerus $\mathrm{Nm}\,k(\alpha)$ dividi possit: $p^{n\delta}$, ubi δ divisor ipsius $\lambda-1$ est is, ad quem p (mod. λ) pertinet. Iam in § 5 probavimus ista statuta condicione eaque addita, ut productum πp *) discerpi possit in δ factores complexos coniunctos, ita ut $\mathrm{Nm}\,p(\varepsilon)=\pi p$ sit, aequationem locum habere:

$$\text{(III.)}\qquad \pi^n k(\alpha) = f(\alpha).p(\varepsilon)^m.p(\varepsilon_1)^{m_1}\ldots,$$

ubi $m+m_1+\cdots=n$ esse debet. Iam numero $\mathrm{Nm}\,f(\alpha)$ nullum amplius factorem p contineri patet, ideoque exstare numerum x talem, ut sit $x.\mathrm{Nm}\,f(\alpha)\equiv 1$ (mod. p^a). Unde cum unitas $r^{\frac{\pi^n k(\alpha)}{p^a}}$ integra sit, unitatem quoque hanc:

$$r^{\frac{p(\varepsilon)^m.p(\varepsilon_1)^{m_1}\ldots}{p^a}} = s$$

integram esse colligimus, atque ex hac ipsa illam unitatem datam $r^{\frac{k(\alpha)}{p^a}}$ deduci posse facile intelligitur. Posito enim y numero tali, ut sit $y\pi^n\equiv 1$ (mod. p^a), ex aequatione (III) sequitur congruentia:

$$yf(\alpha).p(\varepsilon)^m.p(\varepsilon_1)^{m_1}\cdots\equiv k(\alpha)\ (\mathrm{mod.}\,p^a)$$

sive aequatio:

$$yf(\alpha).p(\varepsilon)^m.p(\varepsilon_1)^{m_1}\cdots = k(\alpha)+p^a.\varphi(\alpha),$$

$$\text{unde}\quad s^{yf(\alpha)} = r^{\frac{k(\alpha)}{p^a}}.r^{\varphi(\alpha)}\quad\text{sive}\quad r^{\frac{k(\alpha)}{p^a}} = s^{yf(\alpha)}.r^{-\varphi(\alpha)}.$$

Quod si ad omnes illas unitates (II) adhibemus, sequitur, ut pro illis hae accipi possint unitates:

$$\text{(IV.)}\quad r^{\frac{p(\varepsilon)^m.p(\varepsilon_1)^{m_1}\ldots}{p^a}},\quad r^{\frac{q(\varepsilon)^m.q(\varepsilon_1)^{m_1}\ldots}{q^a}},\quad \ldots .$$

Qua in serie unitatum, si quae iisdem gaudent denominatoribus, eas hac ratione in unam conflare possumus. Sint datae:

$$r^{\frac{p(\varepsilon)^m.p(\varepsilon_1)^{m_1}\ldots}{p^a}},\quad r^{\frac{p(\varepsilon)^n.p(\varepsilon_1)^{n_1}\ldots}{p^a}}$$

---

*) Numerus π talis eligendus, ut sit ad p primus, id quod tantum pro certis numerorum $\mathrm{Nm}(\varepsilon-\varepsilon_r)$ factoribus fieri nequit (v. § 5). His numeris vero methodus supra exhibita facili negotio adaptatur.

sitque complexus factorum $p(\varepsilon)$ utrique numeratori communium $f(\varepsilon)$, ita ut existant aequationes:

$$p(\varepsilon)^m.p(\varepsilon_1)^{m_1}\cdots = f(\varepsilon).p(\varepsilon_h)^v.p(\varepsilon_{h'})^{v'}\cdots = f(\varepsilon).\varphi(\varepsilon),$$
$$p(\varepsilon)^n.p(\varepsilon_1)^{n_1}\cdots = f(\varepsilon).p(\varepsilon_k)^w.p(\varepsilon_{k'})^{w'}\cdots = f(\varepsilon).\psi(\varepsilon),$$

ubi nullum k nulli h aequivalere potest. Quodsi numeri $i, i'\ldots$ tales sunt, ut coniuncti cum ipsis k et h seriem indicum 1, 2, ... $\frac{\lambda-1}{\delta}$ expleant, atque ponitur:

$$\varphi(\varepsilon)+\psi(\varepsilon).p(\varepsilon_i)p(\varepsilon_{i'})\cdots = \chi(\varepsilon),$$

in numero $\mathrm{Nm}\chi(\varepsilon)$ factor p inesse nequit, id quod ratione supra (§ 4) exhibita probari potest. Quare numerus exstat x, qui congruentiae satisfaciat: $x.\mathrm{Nm}\chi(\varepsilon)\equiv 1 \pmod{p^a}$. Deinde cum unitates:

$$r^{\frac{f(\varepsilon)\varphi(\varepsilon)}{p^a}} \quad \text{et} \quad r^{\frac{f(\varepsilon).\psi(\varepsilon)}{p^a}} \quad \text{ideoque} \quad r^{\frac{f(\varepsilon)\chi(\varepsilon)}{p^a}}$$

integrae sint, ope illius congruentiae $x.\mathrm{Nm}f(\varepsilon)\equiv 1 \pmod{p^a}$ etiam unitatem $r^{\frac{f(\varepsilon)}{p^a}}$ integram esse colligimus, ex qua quidem illas duas superiores deduci posse plane in promptu est.

Iam si quae exstant unitates seriei IV, quarum exponentium denominatores diversae potestates eiusdem numeri primi sunt, eas quoque in unam conflari posse hoc modo probamus. Sint datae unitates integrae:

$$r^{\frac{\varphi(\varepsilon)}{p^a}}, \quad r^{\frac{\psi(\varepsilon)}{p^b}},$$

ubi $b < a$. Fractionis $\frac{\psi(\varepsilon)}{p^b}$ et numeratore et denominatore numero πp^{a-b} multiplicatis obtinemus:

$$\frac{\psi(\varepsilon)}{p^b} = \frac{p(\varepsilon_1)^{a-b}p(\varepsilon_2)^{a-b}\ldots\psi(\varepsilon)}{\pi^{a-b}p^a} = \frac{\chi(\varepsilon)}{\pi^{a-b}p^a}.$$

Iam unitates $r^{\frac{\varphi(\varepsilon)}{p^a}}$ et $r^{\frac{\chi(\varepsilon)}{p^a}}$ methodo modo exhibita in unam possunt conflari, ex qua illas duas derivare licet. Ab hac vero unitate $r^{\frac{\chi(\varepsilon)}{p^a}}$ illa data $r^{\frac{\psi(\varepsilon)}{p^b}}$ facile deducitur. Est enim

$$r^{\frac{\chi(\varepsilon)}{p^a}} = r^{\pi^{a-b}\frac{\psi(\varepsilon)}{p^b}},$$

unde si x est numerus talis, ut sit

$$x.\pi^{a-b} \equiv 1 \ (\text{mod.} p^b) \quad \text{sive} \quad x\pi^{a-b} = 1 + kp^b,$$

erit:

$$r^{x.\frac{\chi(\varepsilon)}{p^a}} . r^{-k\psi(\varepsilon)} = r^{\frac{\psi(\varepsilon)}{p^b}}.$$

Ex quibus dictis patet, loco illarum unitatum (I), vel (II), vel (IV) accipi posse unitates quasdam:

$$\text{(V.)} \quad r^{\frac{k(\alpha)}{p^a}}, \quad r^{\frac{k'(\alpha)}{q^b}}, \quad \ldots,$$

in quibus p, q, ... numeri sint primi inter se diversi, quaeque coniunctae cum ipsis r ad repraesentandas omnes unitates sufficiant. Iam probaturi sumus has ipsas unitates conflari posse in hanc:

$$r_1^{\frac{k(\alpha)}{p^a} + \frac{k'(\alpha)}{q^b} + \frac{k''(\alpha)}{t^c} + \ldots} = s_1.$$

Quam enim unitatem integram esse elucet, atque unitates illas (V) ope unitatum r_1, r_2, ... $r_{\lambda-1}$ ex unitate s deduci posse hoc modo probatur. Cum productum $q^b.t^c\ldots$ ad ipsum p primum sit, numerus inveniri potest x talis, ut sit:

$$x.q^b.t^c\ldots \equiv 1 \ (\text{mod.} p^a) \quad \text{sive} \quad x.q^b.t^c\ldots = 1 + np^a,$$

quare erit

$$s^{x.q^b.t^c\ldots} = r_1^{\frac{k(\alpha)}{p^a}} . r_1^{nk(\alpha) + t^c\ldots k'(\alpha) + \ldots},$$

unde unitatem $r_1^{\frac{k(\alpha)}{p^a}}$ re vera potestatibus integris unitatum r et s exprimi posse manifestum est. Cuius explicationis summam hoc modo exhibere possumus: Acceptis quibuslibet unitatibus coniunctis r_1, r_2, ... $r_{\lambda-1}$, semper inveniri potest systema unitatum coniunctarum s_1, s_2, ... $s_{\lambda-1}$ tale, ut omnes unitates integris istarum unitatum r et s potestatibus exprimi liceat.

Iam cum summam tam determinatam neque de numero neque de natura unitatum fundamentalium casu generali huc usque consequi potuerimus, quam paragraphis 14 et 15 suppositione illa speciali explicavimus, relictis iis, quae insuper his methodis derivari possunt, si unitates „r“ certa quadam ratione eliguntur, ad casum eum transeamus, in quo λ numerus est compositus.

§ 18.

Nostra methodus cum eo nitatur, quod istas symbolicas exponentium expressiones ratione numerorum re vera complexorum tractavimus, etiam casu quo λ numerus est compositus, tales instituamus unitates, ut his adiumentis

uti possimus. Quem ad finem sit „d“ aliquis ipsius λ divisor, qui factores primos p q, ... contineat, atque „r“ unitas illa in § 9 memorata; ostendamus exstare unitates s_1, s_2, ... eiusmodi, ut his aequationibus satisfaciant:

$$\text{(I.)} \qquad s_k = s_{d+k} = s_{2d+k} = \cdots = s_{(\delta-1)d+k} \quad \text{posito} \quad \delta d = \lambda,$$

praetereaque his:

$$\text{(II.)} \quad \begin{cases} s_k . s_{\frac{d}{p}+k} . s_{2\frac{d}{p}+k} \cdots s_{(p-1)\frac{d}{p}+k} = 1, \\ s_k . s_{\frac{d}{q}+k} . s_{2\frac{d}{q}+k} \cdots s_{(q-1)\frac{d}{q}+k} = 1, \\ \vdots \qquad\qquad \vdots \qquad\qquad \vdots , \end{cases}$$

sive his quae illis aequivalent, si $\log s_k = \sigma_k$ et α radix quaevis aequationis $x^\lambda = 1$ ponitur:

$$\text{(III.)}\ \sigma_1+\sigma_2\alpha+\cdots+\sigma_\lambda\alpha^{\lambda-1} = \sigma_{d+1}+\sigma_{d+2}\alpha+\cdots+\sigma_d\alpha^{\lambda-1}, \text{ ergo } = \alpha^{-d}(\sigma_1+\sigma_2\alpha+\cdots+\sigma_\lambda\alpha^{\lambda-1})$$

atque his:

$$\text{(IV.)} \quad \begin{cases} (\sigma_1+\sigma_2\alpha+\cdots+\sigma_\lambda\alpha^{\lambda-1})(1+\alpha^{-\frac{d}{p}}+\alpha^{-2\frac{d}{p}}+\cdots+\alpha^{-(p-1)\frac{d}{p}}) = 0, \\ (\sigma_1+\sigma_2\alpha+\cdots+\sigma_\lambda\alpha^{\lambda-1})(1+\alpha^{-\frac{d}{q}}+\alpha^{-2\frac{d}{q}}+\cdots+\alpha^{-(q-1)\frac{d}{q}}) = 0, \\ \vdots \qquad\qquad \vdots \qquad\qquad \vdots . \end{cases}$$

Quae ipsae condiciones explentur, si expressio $\sigma(\alpha)$ pro quovis ipsius α valore exceptis iis, qui radices unitatis d^{tae} primitivae sunt, evanescit. Quod si fit, aequatio (III), quae pro valoribus ipsius α aequationi $\alpha^d = 1$ sufficientibus re ipsa expletur, etiam pro reliquis ipsius α valoribus locum tenet. Deinde aequationes (IV), quae pro iis tantum ipsius α valoribus, qui radices primitivae d^{tae} sunt, re ipsa explentur, etiam pro reliquis ipsius α valoribus valent. Iam ponamus:

$$\text{(V.)} \qquad s_1 = r_1^{a_1+a_2\alpha+\cdots+a_{\lambda-1}\alpha^{\lambda-2}} = r_1^{a_1} r_2^{a_2} \cdots r_{\lambda-1}^{a_{\lambda-1}},$$

ubi

$$a_1+a_2\alpha+\cdots+a_{\lambda-1}\alpha^{\lambda-2}$$
$$= (1+\alpha^d+\cdots+\alpha^{(\delta-1)d})(1+\alpha+\alpha^2+\cdots+\alpha^{\frac{d}{p}-1})(1+\alpha+\alpha^2+\cdots+\alpha^{\frac{d}{q}-1})\cdots .$$

Ex qua aequatione numeri a_1, a_2, ... ita sunt determinandi, ut explicato producto dextrae partis eoque solius aequationis $\alpha^\lambda = 1$ ope reducto singularum ipsius α potestatum coefficientes quantitatibus a_1, a_2... aequales ponantur, sive hoc modo, ut positis in aequatione (V) singulis ipsius α valoribus ex his ($\lambda-1$) aequationibus illae ($\lambda-1$) quantitates „a“ determinentur. — Unitates „s“ sic definitas illis aequationibus (I), (II), (III), (IV) satisfacere

iam probaturi sumus. — Ex illa enim aequatione (V) sequitur modo in § 10 tradito, ut sit:

$$\sigma_1+\sigma_2\alpha+\cdots+\sigma_\lambda\alpha^{\lambda-1} = a(\alpha^{-1})(\varrho_1+\varrho_2\alpha+\cdots+\varrho_\lambda\alpha^{\lambda-1})$$

pro quavis radice α. Cum vero expressio:

$$a(\alpha^{-1}) = \frac{1-\alpha^{-\lambda}}{1-\alpha^{-d}}\cdot\frac{1-\alpha^{-\frac{d}{p}}}{1-\alpha^{-1}}\cdot\frac{1-\alpha^{-\frac{d}{q}}}{1-\alpha^{-1}}\cdots$$

pro omnibus ipsius α valoribus exceptis radicibus d^{tis} primitivis evanescat, etiam expressionem $\sigma(\alpha)$ hanc ipsam habere proprietatem ideoque unitates „s“ illis condicionibus sufficere patet.

Quaecunque unitates illis aequationibus (I), (II), (III), (IV) satisfaciunt classem efficiunt unitatum eam, quam ad divisorem „d“ pertinere dicimus. Iam primum unitates eiusdem classis inter se comparabimus, et quidem omnes potestatibus vel integris vel fractis unius systematis unitatum coniunctarum exprimi posse probabimus. Etenim sint unitates aliquae ad divisorem d pertinentes hae: $f_1, f_2, \ldots f_d$; designentur deinde valores absoluti logarithmorum harum quantitatum signis: $\varphi_1, \varphi_2, \ldots \varphi_d$; hoc aequationum systema semper solvi potest:

$$\text{(VI.)}\quad \begin{cases} \varphi_1 = n_1\sigma_1+n_2\sigma_2+\cdots+n_k\sigma_k, \\ \varphi_2 = n_1\sigma_2+n_2\sigma_3+\cdots+n_k\sigma_{k+1}, \\ \vdots \qquad\qquad \vdots \qquad\qquad \vdots \\ \varphi_d = n_1\sigma_d+n_2\sigma_1+\cdots+n_k\sigma_{k-1}, \end{cases}$$

ubi indeterminatae sunt quantitates $n_1, n_2, \ldots n_k$ atque numerus harum quantitatum, litera k designatus, numerus ille est, quem *Gauss* signo $\varphi(d)$ denotat, i. e. numerus numerorum ad ipsum „d“ primorum eoque minorum. Designante w radicem aequationis $w^d = 1$ pro qualibet hac radice w, ratione in § 9 exhibita prodit aequatio:

$$\text{(VII.)}\quad \varphi_1+\varphi_2 w+\cdots+\varphi_d w^{d-1} = (n_1+n_2 w^{-1}+\cdots+n_k w^{k-1})(\sigma_1+\sigma_2 w+\cdots+\sigma_d w^{d-1}).$$

Quam aequationem pro omnibus radicibus w non primitivis re ipsa expleri ex eo elucet, quod his casibus et $\varphi(w)$ et $\sigma(w)$ evanescunt, cum et unitates f et unitates s in classe ad divisorem d pertinente insint*). — Singuli ipsius w valores primitivi totidem aequationes praebent formae (VII), quarum igitur numerus k numero indeterminatarum aequalis est. Ut igitur indeterminatas ex iis determinari posse ostendamus, tantummodo determinantem systematis

*) v. quae supra indicata sit unitatum ad classem pertinentium proprietas.

illius non evanescere probandum est. Determinans autem cum sit:

$$\sigma(w).\sigma(w^h).\sigma(w^{h'})\ldots,$$

designantibus h, h', ... systema numerorum inter se incongruorum ad ipsum d primorum, aliquis factor $\sigma(w^h)$ evanescere deberet, ideoque foret:

$$\sigma_1+\sigma_2 w+\sigma_3 w^2+\cdots+\sigma_d w^{d-1} = 0$$

pro aliqua radice primitiva w, sive ratione habita aequationum (I) nec non aequationis huius: $\alpha^\delta = w$ esse deberet:

$$\sigma_1+\sigma_2\alpha^\delta+\sigma_3\alpha^{2\delta}+\cdots+\sigma_\lambda\alpha^{\delta(\lambda-1)} = 0$$

pro aliqua radice primitiva α. — Iam cum sit secundum aequationem (V):

$$\sigma_1+\sigma_2\alpha^\delta+\cdots+\sigma_\lambda\alpha^{\delta(\lambda-1)} = (\varrho_1+\varrho_2\alpha^\delta+\cdots+\varrho_\lambda\alpha^{\delta(\lambda-1)})(a_1+a_2\alpha^\delta+\cdots),$$

esse deberet:

$$\varrho(\alpha^\delta)(a_1+a_2\alpha^\delta+\cdots) = 0,$$

sive substituto ipsius $a(\alpha^\delta)$ valore et posito $\alpha^\delta = w$:

$$\varrho(\alpha^\delta).\delta.\frac{1-w^{\frac{d}{p}}}{1-w}.\frac{1-w^{\frac{d}{q}}}{1-w}\cdots = 0,$$

id quod fieri nequit, cum nullum factorem $(1-w^{\frac{d}{p}})$, ..., designante w radicem *primitivam* d^{tam}, evanescere pateat, neque factorem $\varrho(\alpha^\delta)$ nihilo aequivalere posse supra in § 9 demonstratum sit.

Iam cum probaverimus, quamvis unitatem ad ipsum „d" pertinentem potestatibus ipsorum s repraesentari posse*), exponentes harum potestatum non irrationales esse ex eo elucet, quod, cum unitates s potestatibus integris unitatum r expressae sint, etiam unitates quaedam potestatibus ipsorum „r" irrationalibus repraesentari possent, id quod fieri non posse in § 13 demonstravimus. Quare forma generalis unitatum ad divisorem „d" pertinentium erit:

$$s_1^{\frac{m_1}{n}}.s_2^{\frac{m_2}{n}}\ldots s_k^{\frac{m_k}{n}}$$

sive:

$$s_1^{\frac{1}{n}(m_1+m_2 w+\cdots+m_k w^{k-1})}$$

designantibus n, m_1, m_2, ... numeros integros reales.

In quibus unitatibus exponentes symbolicos tanquam veros numeros complexos tractare possumus, quia omnes eorum reductiones aequationibus nituntur:

*) Nempe si in aequationibus (VI) a logarithmis ad numeros transeas.

$$\begin{cases} 1+w^{\frac{d}{p}}+w^{2\frac{d}{p}}+\cdots+w^{(p-1)\frac{d}{p}} = 0, \\ 1+w^{\frac{d}{q}}+w^{2\frac{d}{q}}+\cdots+w^{(q-1)\frac{d}{q}} = 0, \\ \vdots \qquad \vdots \qquad \vdots \end{cases}$$

et

$$1+w+w^2+\cdots+w^{d-1} = 0,$$

cumque re vera sit:

$$s^{1+w^{\frac{d}{p}}+\cdots+w^{(p-1)\frac{d}{p}}} = s_1.s_{\frac{d}{p}+1}\ldots s_{(p-1)\frac{d}{p}+1} = 1 = s_1^0 \quad \text{etc.}$$

nec non:

$$s_1^{1+w+\cdots+w^{d-1}} = s_1.s_2\ldots s_d = 1 = s_1^0.$$

§ 19.

Respectu habito eorum, quae in § 7 cum explicata tum indicata sint, atque posito „λ" numerum esse eiusmodi, ut quivis numerus primus formae $k\lambda+r$ in n factores complexos, compositos e radicibus unitatis λ^{tis}, discerpi possit, si statuamus $g, g', g'', \ldots$ resp. numerorum $p^a, q^b, t^c, \ldots$ radices primitivas,

$$\lambda = p^a.q^b.t^c\ldots, \quad r \equiv \frac{\lambda}{p^a}\cdot g^h + \frac{\lambda}{q^b}\cdot g'^{h'} + \frac{\lambda}{t^c}\, g''^{h''} + \cdots \pmod{\lambda},$$

$$n = h.h'.h''\ldots{}^{*}),$$

omnino eadem qua in § 15 usi sumus ratione probatur, exstare in quavis classe unitatem u, cuius potestatibus integris complexis omnes unitates ad eandem classem pertinentes repraesentari possint. Cumque quivis numerus complexus integer ex unitatis radicibus d^{tis} compositus ad expressionem $\varphi(d)$ terminorum integram redigi possit**), $\varphi(d)$ unitates coniunctas exstare patet, quarum potestatibus integris omnes unitates ad divisorem d pertinentes exprimi possint.

Iam eadem qua in § 16 usi sumus ratione probari potest, designante „u" unitatem fundamentalem classis ad ipsum d pertinentis, omnes reliquas eiusdem classis unitates fundamentales easque solas forma contineri: $u^{m(w)}$, si $m(w)$ numerus est talis, ut $\text{Nm}\, m(w) = 1$. Etiamque unitates non coniunctae statui possunt fundamentales multitudinis $\varphi(d)$, et quidem numerus unitatum diversarum, quae statui possunt, fundamentalium coniunctarum erit

*) Numeri $h, h', \ldots$ resp. multipla numerorum $p^{a-1}, q^{b-1}, \ldots$ esse debent.

**) v. § 7.

infinitus, dummodo $\varphi(d) > 2$, ergo $d \geqq 8$, numerus vero unitatum fundamentalium non coniunctarum erit infinitus, quando $\varphi(d) \geqq 2$, ergo $d > 2$.

Denique omissa illa suppositione, qua statuitur, omnem numerum primum formae $k\lambda+r$ in n factores complexos discerpi posse, ratione illa in § 17 exhibita demonstrari potest: dato quocunque systemate unitatum coniunctarum ad classem aliquam pertinentium*), semper existere aliud systema, quo alteri adiuncto cunctae eiusdem classis unitates repraesentari possint. Et quidem secundum supra adnotata utrarumque unitatum tantummodo $\varphi(d)^{\text{nis}}$ opus erit.

Iam etiam probemus numerum unitatum fundamentalium ipso $\varphi(d)$ minorem non sufficere ad repraesentandas omnes unitates eiusdem classis. Quem ad finem sint unitates quaedam fundamentales: $f, f', f'', \ldots$, itaque illas quoque unitates „s“ potestatibus harum f integris repraesentari posse oportet. Quare sit posito $\log f = \varphi$, $\log f' = \varphi'$, ... et $k = \varphi(d)$:

$$\begin{cases} \sigma_1 = a_1\varphi + b_1\varphi' + c_1\varphi'' + \cdots, \\ \sigma_2 = a_2\varphi + b_2\varphi' + c_2\varphi'' + \cdots, \\ \vdots \qquad \vdots \qquad \vdots \\ \sigma_k = a_k\varphi + b_k\varphi' + c_k\varphi'' + \cdots. \end{cases}$$

Cum vero numerus ipsorum f itaque ipsorum φ sit $\leqq k-1$, his ipsis eliminatis certe una restabit aequatio formae huiusce:

$$\text{(I.)} \qquad n_1\sigma_1 + n_2\sigma_2 + \cdots + n_k\sigma_k = 0,$$

in qua aequatione n_1, n_2, ... numeri esse debent integri atque non omnes nihilo aequales. Id quod fieri non posse sequentibus probatur. Ex aequatione enim (I) sequitur: $s_1^{n_1}s_2^{n_2}\ldots s_k^{n_k} = 1$, unde mutatis periodis iis, quae unitatibus „s“ continentur, oritur systema aequationum:

$$\begin{cases} s_1^{n_1}s_2^{n_2}\ldots s_k^{n_k} = 1, \\ s_2^{n_1}s_3^{n_2}\ldots s_{k+1}^{n_k} = 1, \\ \vdots \qquad \vdots \qquad \vdots, \end{cases}$$

ex quo ope formulae (IV) § 9 deducimus aequationem:

$$(n_1 + n_2 w^{-1} + \cdots + n_k w^{-k+1})(\sigma_1 + \sigma_2 w + \cdots + \sigma_d w^{d-1}) = 0$$

pro qualibet d^{ta} radice unitatis w. Cum autem factorem alterum pro nulla

---

*) Ea tantum condicione, ut expressio illa $\sigma(w)$ pro nullo valore ipsius w primitivo evanescat. v. § 18.

radice w primitiva evanescere supra (§ 18) demonstratum sit, factor prior pro his omnibus k valoribus ipsius w evanescere deberet; id quod (nisi $n_1 = n_2 = \cdots = 0$) fieri non posse ex § 7 colligitur.

§ 20.

Iam quid ex hac singularum classium disquisitione pro universis unitatibus colligi possit, inquiramus. Quodsi supponimus numerum λ illa virtute, initio § 19 memorata, gaudere, ea ipsa proprietate divisores quoque ipsius λ praeditos esse patet. Hoc igitur casu pro quolibet divisore „d" exstant quaedam unitates fundamentales coniunctae, quarum $\varphi(d)$ ad repraesentandas omnes huius classis unitates sufficiunt; quae designentur notis $u_{d,1}$, $u_{d,2}$, ..., earumque logarithmi sint $v_{d,1}$, $v_{d,2}$, ...

Sit „r" unitas aliqua, atque formetur ex ea unitas classis ad divisorem „d" pertinentis illa ipsa ratione, qua initio § 18 usi sumus. Sitque haec unitas „s", ita ut habeamus servata designatione illic adhibita:

$$r_1^{a_1} r_2^{a_2} \ldots r_{\lambda-1}^{a_{\lambda-1}} = r_1^{a(\alpha)} = s_1.$$

Sed esse debet

$$s_1 = u_{d,1}^{n_1} . u_{d,2}^{n_2} \ldots u_{d,k}^{n_k}$$

designantibus n_1, n_2... numeros quosdam integros. Itaque habemus aequationem:

$$\text{(I.)} \quad \sigma_1 + \sigma_2 w + \cdots + \sigma_d w^{d-1} = (n_1 + n_2 w^{-1} + \cdots + n_k w^{-(k-1)})(v_{d,1} + v_{d,2} w + \cdots + v_{d,d} w^{d-1})$$

ratione saepe usitata pro qualibet radice w aequationis $w^d = 1$. Deinde est:

$$\text{(II.)} \quad \sigma_1 + \sigma_2 \alpha \cdots + \sigma_\lambda \alpha^{\lambda-1} = a(\alpha^{-1})(\varrho_1 + \varrho_2 \alpha + \cdots + \varrho_\lambda \alpha^{\lambda-1})$$

pro quaque radice unitatis λ^{ta}. Substituta igitur pro α radice w obtinemus:

$$a(w^{-1})(\varrho_1 + \varrho_2 w + \cdots + \varrho_\lambda w^{\lambda-1}) = \sigma_1 + \sigma_2 w + \cdots + \sigma_\lambda w^{\lambda-1},$$

atque per aequationem (I) aliquanto mutatam:

$$\text{(III.)} \quad \begin{cases} a(w^{-1})(\varrho_1 + \varrho_2 w + \cdots + \varrho_\lambda w^{\lambda-1}) \\ = (n_1 + n_2 w^{-1} + \cdots + n_k w^{-(k-1)})(v_{d,1} + v_{d,2} w + \cdots + v_{d,\lambda} w^{\lambda-1}). \end{cases}$$

Quotiescunque igitur $n(w^{-1})$, numero $a(w^{-1})$ divisus, residuum habet $c(w^{-1})$, ita ut

$$n(w^{-1}) = m(w^{-1}) a(w^{-1}) + c(w^{-1})$$

sit (designante w radicem primitivam), habemus aequationem:

$$a(w^{-1})(\varrho_1 + \varrho_2 w + \cdots) = a(w^{-1}) m(w^{-1})(v_{d,1} + v_{d,2} w + \cdots) + c(w^{-1})(v_{d,1} + v_{d,2} w + \cdots),$$

atque si ponimus unitatem:

$$r_1 . u_{d,1}^{-m_1} . u_{d,2}^{-m_2} \dots u_{d,k}^{-m_k} = t_1$$

et $\log . t_1 = \tau_1$, erit:

$$a(\alpha^{-1})(\tau_1 + \tau_2 \alpha + \dots + \tau_\lambda \alpha^{\lambda-1}) = c(\alpha^{-1})(v_{d,1} + v_{d,2} \alpha + \dots + v_{d,\lambda} \alpha^{\lambda-1})$$

pro quoque ipsius α valore, qui radicem d^{tam} primitivam praebet. Pro omnibus reliquis ipsius α valoribus erit:

$$\tau_1 + \tau_2 \alpha + \dots + \tau_\lambda \alpha^{\lambda-1} = \varrho_1 + \varrho_2 \alpha + \dots + \varrho_\lambda \alpha^{\lambda-1},$$

cum pro his ipsius α valoribus sit $v_{d,1} + v_{d,2} \alpha + \dots = 0$.

Unde elucet, quamvis unitatem „r" ope unitatum „u" ad unitatem „t" reduci posse talem, ut si unitas classis ad „d" pertinentis ratione supra indicata ex ea formetur atque potestate ipsius „u" complexa repraesentetur, exponens certo quodam residuorum systemate modulo $a(w)$ contineatur*). Hinc tanquam corollarium sequitur, ut si tales tantum unitates existant, quarum exponentes illi cuncti residua nihilo aequalia habeant, quascunque unitates integris ipsorum „u" potestatibus exprimere liceat, itaque numerus unitatum fundamentalium sit:

$$\varphi(\lambda) + \dots + \varphi(d) + \dots = \lambda - 1$$

secundum notum illud theorema.

Statutis certis quibusdam residuorum systematis modulis $a(w)$, $a'(w')$, ... pro singulis ipsius λ divisoribus, sit unitas „r" eiusmodi, ut exponentes, ad quos pertinent unitates classium ex illa „r" formatae, pro singulis $a(w)$ residuis quibusdam ex istis systematis aequales sint; tum brevitatis causa seriem quandam residuorum ad unitatem „r" pertinere dicemus. Iam primum ex illis supra dictis concludimus, cunctas unitates unitatibus „u" et unitatibus „r" repraesentari posse.

Deinde supponamus divisores ipsius λ certo aliquo ordine dispositos:

$$d_1, \; d_2, \; \dots \; d_i;$$

sint porro unitates „r" tales, ut residua, quae ad eas respectu divisoris d_1 pertineant, non evanescant; sint unitates „s" tales, ut residuis respectu d_1 evanescentibus residua, quae ad eas respectu divisoris d_2 pertineant, non evanescant etc. Inter has unitates r, s, t, ... omnes illas, quae supra ipso „r" denotatae sunt, inveniri apertum est. Deinde adnotamus, pro divisore

*) Sic supra pro unitate „r", ad quam exponens $k(w)$ pertinebat, ad unitatem „t" reducta est, ad quam exponens $c(w)$, qui est residuum ipsius $n(w)$ modulo $a(w)$, pertinet.

ultimo tales unitates existere non posse. Tum enim residua respectu omnium divisorum, excepto ipso d_i, evanescere deberent ideoque, posito illam unitatem z eiusque logarithmum ζ esse, aequatio

$$\zeta_1+\zeta_2\alpha+\cdots+\zeta_\lambda\alpha^{\lambda-1} = 0$$

pro omnibus ipsius α valoribus exceptis radicibus d_i^{tis} primitivis locum habere deberet. Itaque unitas z in ipsa classe ad divisorem d_i pertinente inest (v. § 18) atque in aequatione:

$$a(w^{-1})(\zeta_1+\zeta_2 w+\cdots+\zeta_\lambda w^{\lambda-1}) = (n_1+n_2 w^{-1}+\cdots)(v_{d_i,1}+v_{d_i,2}w+\cdots),$$

ubi w est radix d_i^{ta} primitiva, numerus $n(w)$ ipso $a(w)$ dividi posse deberet, propterea que residuum respectu divisoris d_i quoque evanesceret.

Iam unitates „r" inter se reducendae sunt. Primum, si quae existant, ad quas idem residuum respectu ipsius d_1 pertineat, e. g. r et r', pro his accipi possunt unitates r et $\frac{r}{r'}$, quarum alteram ad genus unitatum „s" (vel inter ipsas t, ...) referendam esse patet, quippe quae eius residuum respectu d_1 evanescat. Unde concludimus, quaecunque unitates r eodem residuo respectu d_1 gaudeant, ex eis unam tantum eligendam esse, cum ceterae ope huius et unitatum s, t, ... repraesentari possint. — Deinde sit $n(w)$ residuum alicuius „r" respectu d_1 (ubi w radix primitiva d_1^{ta}), sitque $\varphi(w)$ factor communis maximus numerorum $n(w)$ et illius $a(w)$, ita ut sit

$$n(w) = \varphi(w).m(w),$$

numerum invenire licet $\psi(w)$ talem, ut sit

$$m(w)\psi(w) \equiv 1 \pmod{a(w)}\ ^{*}),$$

ergo

$$n(w)\psi(w) \equiv \varphi(w) \pmod{a(w)}.$$

Itaque cum unitas $r_1^{\psi(\alpha)}$ quoque integra sit, unitas existit, cuius residuum respectu d_1 ipse numerus $\varphi(w)$ est. Quae si litera r' designatur, erit $r'^{m(\alpha)}$ unitas, cuius residuum respectu d_1 numerus $n(w)$, quae igitur secundum supra dicta pro illa unitate r accipi potest. Hinc sequitur, ut loco omnium earum unitatum, quarum residua eundem factorem communem maximum $\varphi(w)$ cum numero $a(w)$ habeant, unam tantum, cuius residuum ipse hic numerus $\varphi(w)$ sit, accipere liceat.

---

*) Cf. § 4 et § 7.

Sint unitatum r et r' residua respectu d_1 numeri $\varphi(w)$ et $\psi(w)$, qui uterque numerum illum $a(w)$ metiens supponi potest. Tum erit factor communis maximus numerorum

$$m(w)\varphi(w)+n(w)\psi(w), \quad a(w)$$

ipse factor communis numerorum $\varphi(w)$ et $\psi(w)$. Positis enim $m(w)$, $n(w)$ numeros esse tales, ut sit

$$m(w)\varphi(w)+n(w)\psi(w)\equiv\chi(w) \pmod{a(w)},$$

ubi $\chi(w)$ factor est communis maximus ipsorum $\varphi(w)$ et $\psi(w)$, illa sententia elucet. Cumque etiam $r^{m(w)}.r'^{n(w)}$ unitas sit integra eaque talis, ut residuum respectu d_1 sit $\chi(w)$, hanc ipsam unitatem, ex qua ope unitatum $s, t, \ldots$ unitates illae (r, r') derivari possunt, loco duarum unitatum r, r' accipere licet. Quaecunque igitur unitates variorum respectu d_1 residuorum existunt, semper una talis pro iis accipi potest, cuius residuum respectu d_1 factor omnium residuorum communis maximus sit. Et, si respicimus supra dicta, pro hac ipsa talis statui potest unitas, ut residuum respectu d_1 sit factor ipsius $a(w)$.

Quae cum de unitatibus r exposuerimus, ad unitates $s, t, \ldots$ adhibere liceat, concludimus, praeter unitates „u" ad repraesentandas omnes unitates his tantum opus esse: unitate quadam „r" (cum eius coniunctis), cuius residuum respectu d_1 est factor ipsius $a(w)$; unitate quadam „s", cuius residuum respectu d_2 est factor ipsius $b(w')$ etc. Itaque hanc obtinemus seriem unitatum fundamentalium:

$$\begin{array}{cccccc} u_{d_1}, & u_{d_2}, & u_{d_3}, & \ldots & u_{d_{i-1}}, & u_{d_i}, \\ r, & s, & t, & \ldots & z. & \end{array}$$

Iam si residuum, quod ad unitatem r respectu d_1 pertinet, $\varphi(w)$ ponitur, ita ut sit $a(w)=\varphi(w).\psi(w)$, habemus aequationem:

$$a(w^{-1})(\varrho_1+\varrho_2 w+\cdots) = \varphi(w^{-1})(v_{d_1,1}+v_{d_1,2}w+\cdots)$$

vel

$$\psi(w^{-1})(\varrho_1+\varrho_2 w+\cdots) = v_{d_1,1}+v_{d_1,2}w+\cdots,$$

pro qualibet radice d_1^{ta} primitiva w. Unde patet unitatem $r^{\psi(\alpha)}.u_{d_1,1}^{-1}$ esse talem, ut eius residuum respectu d_1 sit nihilo aequale, eamque igitur unitatibus $u_{d_2}, u_{d_3}, \ldots$ et $s, t, \ldots$ repraesentari posse. Ergo ipsae unitates coniunctae u_{d_1} unitatibus „r" et reliquis utriusque seriei unitatibus expri-

muntur. Inter has vero unitates „r“ eae, quarum index numero $\varphi(d_1)$ maior est, ad priores reducuntur. Sit enim (posito $\varphi(d_1) = k$)

$$x^k + c_{k-1}x^{k-1} + \cdots + c_1 x + c = 0$$

illa aequatio, quarum radices sunt radices unitatis d_1^{tae} primitivae, in qua coefficientem ipsius x^k unitatem esse e forma illius aequationis in § 7 exhibita manifestum est, et fingamus unitatem integram:

$$r_1^{c}.r_2^{c_1}\ldots r_{k-1}^{c_{k-2}}.r_k^{c_{k-1}}.r_{k+1} = x_1,$$

ideoque posito $\log x_i = \xi_i$:

$$(c + c_1\alpha + \cdots + c_{k-1}\alpha^{k-1} + \alpha^k)(\varrho_1 + \varrho_2\alpha + \cdots) = \xi_1 + \xi_2\alpha + \cdots.$$

Cum vero $c(\alpha)$, eaque de re $\xi(\alpha)$, pro illo ipsius α valore $\alpha = w$ evanescat, unitas x_1 unitatibus $u_{d_2}\ldots$ atque unitatibus s, t, ... repraesentari potest. Ergo r_{k+1} unitatibus r_1, r_2, ... r_k et unitatibus utriusque illius seriei reliquis exprimi potest; pariterque r_{k+2} unitatibus r_2, r_3, ... r_{k+1} ideoque unitatibus r_1, r_2, ... r_k et reliquis etc. etc. Itaque pro illis unitatibus „u_{d_1}“ et „r“ tantum accipiendae sunt unitates:

$$r_1, \quad r_2, \quad \ldots \quad r_{\varphi(d_1)}.$$

Simili modo pro unitatibus u_{d_2} et s tantum accipiendae sunt unitates

$$s_1, \quad s_2, \quad \ldots \quad s_{\varphi(d_2)},$$

quia sicuti supra et unitates ceterae cum s_1 coniunctae et unitates „u_{d_2}“ per unitates s_1, s_2, ... $s_{\varphi(d_2)}$ adiunctis illis u_{d_3}, ... t, ... z, exprimi possunt. Denique pro unitatibus $u_{d_{i-1}}$ et z accipiendae sunt unitates

$$z_1, \quad z_2, \quad \ldots \quad z_{\varphi(d_{i-1})},$$

quia his ipsis ope unitatum u_{d_i} illae repraesentari possunt. Habemus igitur tanquam unitates fundamentales, ad repraesentandas omnes unitates sufficientes, has:

$$\begin{array}{llll}
r_1, & r_2, & \ldots & r_{\varphi(d_1)}, \\
s_1, & s_2, & \ldots & s_{\varphi(d_2)}, \\
\vdots & \vdots & & \vdots \\
z_1, & z_2, & \ldots & z_{\varphi(d_{i-1})}, \\
u_{d_i,1}, & u_{d_i,2}, & \ldots & u_{d_i,\varphi(d_i)},
\end{array}$$

quia ceteras cum ipsis u_{d_i} coniunctas unitates „u" illis exprimi posse iam supra adnotavimus. Numerus igitur unitatum fundamentalium erit:

$$\varphi(d_1)+\varphi(d_2)+\cdots+\varphi(d_i) = \lambda-1,$$

eumque numerum ipso $\lambda-1$ minorem esse non posse in § 12 demonstravimus.

Numerus igitur unitatum fundamentalium hic idem est, qui erat casu quo λ numerus primus, sed cum casu generali, tanquam unitates fundamentales semper unitates accipi posse *coniunctas*, non probaverimus, num re vera unitates fundamentales *coniunctae* pro quovis λ existant, in dubio remanet. Haec autem quaestio quanti sit momenti ex eo elucet, quod problema illud Diophanteum (v. § 11) inveniendorum numerorum x, x_1, ... $x_{\lambda-1}$ aequationi

$$\mathrm{Nm}(x\varepsilon+x_1\varepsilon_1+\cdots+x_{\lambda-1}\varepsilon_{\lambda-1}) = \pm 1$$

satisfacientium systematis unitatum fundamentalium *coniunctarum* perfecte solvitur. Nam si omnes unitates forma $u_1^{n(\alpha)}$ sive

$$(\xi\varepsilon+\xi_1\varepsilon_1+\cdots+\xi_{\lambda-1}\varepsilon_{\lambda-1})^{n(\alpha)}$$

continentur, cuncta ipsorum x systemata *functionibus rationalibus integris* illius unius systematis (ξ) repraesentari possunt. Sin vero duorum systematum unitatum coniunctarum opus est, omnia systemata ipsorum x nonnisi duobus systematis (ξ), (ξ') modo rationali exprimi possunt. Quoniam autem in § 17 demonstratum est, acceptis quibuslibet unitatibus coniunctis r_1, r_2, ... $r_{\lambda-1}$ semper inveniri posse alterum systema s_1, s_2, ... $s_{\lambda-1}$ tale, ut omnes unitates integris istarum unitatum r et s potestatibus exprimi liceat, sequitur, ut accepto quolibet systemate x^0, x_1^0, ... $x_{\lambda-1}^0$ alterum systema x', x_1', ... $x_{\lambda-1}'$ inveniri possit tale, ut omnia systemata ipsorum x tanquam functiones rationales integrae illarum 2λ quantitatum x^0, x' repraesentari possint. Sed cum e disquisitionibus illis generalibus Cli. *Lejeune-Dirichlet*, quas supra pagina huius dissertationis secunda*) commemoravimus, tantummodo concludi possit, $\lambda-1$ quantitatum x systemata sive $\lambda(\lambda-1)$ quantitates x ad repraesentanda cuncta ipsorum x systemata sufficere, casu quem in hac dissertatione tractavimus speciali problema Diophanteum, quaestione unitatum complexarum exhibitum, peculiarem ac simpliciorem solutionem admittere bene animadvertendum est.

*) Paginae, quascunque allegavi, ab initio huius dissertationis numerandae sunt.

